# Cyber Mission Analysis

## Mission Analysis for Cyber Operations of Department of Defense

Submitted in compliance with the reporting requirement contained in the Fiscal Year 2014 National Defense Authorization Act section 933(d), Public Law 113-66

**Preparation of this study/report cost the Department of Defense approximately $587,000 for the 2014 Fiscal Year. This includes $15,000 in expenses and $572,000 in DoD labor**

**Generated on 2014 August 21**

**RefID: E-0CD45F6**

## Table of Contents

# I. Executive Summary

This report fulfills the requirement contained in the National Defense Authorization Act (NDAA) for Fiscal Year 2014, Section 933 "Mission Analysis for Cyber Operations of the Department of Defense (DoD)." The Department undertook an accelerated but deliberate process to conduct the analysis, the outcomes of which are contained in this report. The analysis addressed each sub-section of the statute and was fully vetted across the Department. The results of this analysis reflect the Department's current view of its requirements for successful conduct of cyberspace operations, leveraging a Total Force solution. As cyberspace capabilities, force structure, and command and control (C2) constructs evolve, the Department will conduct periodic reviews of its cyberspace requirements and adjust them as necessary.

To complete this comprehensive analysis, the Office of the Secretary of Defense (OSD) conducted a number of consultations with key stakeholders to ensure a transparent process. OSD Cyber Policy solicited input from the Reserve Forces Policy Board, the State Adjutants General, the National Guard Bureau (NGB), the Guard Senior Leadership Council, the Department of Homeland Security (DHS), and States, through the Council of Governors (CoG). Through these engagements, the Services, OSD, the Joint Staff, the National Guard Bureau, U.S. Cyber Command (USCYBERCOM), DHS, and the States provided the data and analysis that form the backbone of this report. This report reflects the Department's current view, and is expected to change as circumstances require. The findings reflect the assessment done to date.

First, the Department assesses there can be advantages to using reserve component (RC) resources for Cyber Mission Force (CMF) missions, such as providing load sharing with active duty forces, providing available surge capacity if authorized to activate, and maintain DoD-trained forces to defend national critical infrastructure, if authorized. Several factors should be considered when determining the CMF force structure and the mix within the Total Force. These factors include 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.

To that end, there are five key recommended ways forward for the Department as it considers the future of DoD cyber operations, discussed in detail in the "Department's Assessment" section.

1. National Guard personnel could focus on coordinate, train, advise, and assist (C/TAA) support roles when directed by their Governor or Adjutant General if in State active duty status or, if authorized by DoD, in Title 32, U.S. Code, status.
2. The Services' proposed plans to integrate approximately 2,000 RC personnel into the cyber force structure adequately addresses the opportunity for surge support and additional Service Cyber Protection Team (CPT) support in the near-term.
3. Cyber forces require consideration of a persistent training environment.
4. Because there is no command and control over National Guard cyber forces in Title 32 or State active duty status, policies and processes must be clarified to ensure unity of effort by DoD forces and State National Guard forces.
5. The Military Departments/Services may require additional flexibility in civilian hiring authorities.

Although the Department assesses these are the right steps to date, it recognizes that additional analysis is necessary, and will reassess and adjust in Fiscal Year 2016 and in other future budget submissions, once the CMF is well on its way to being fully manned, trained, and equipped to ensure that we have the most effective workforce to conduct DoD cyber operations.

Cyber is a dynamic domain, and, therefore, additional research needs to be completed to determine a number of elements directed in the reporting requirements, including better understanding civilian requirements, understanding the exact equipping needs of the CMF, and the appropriateness of hiring on a temporary basis part-time, non-dual status technicians. It is expected the Department's assessment will mature, and the approach will adapt as this operational domain matures, our forces become operational, and the threat landscape evolves.

# II. Current State

## Threat Landscape

In 2014, the Director of National Intelligence identified cyber threats first among the strategic threat to the United States, surpassing terrorism. Hostile actors use cyberspace as an asymmetric capability to strike the U.S. homeland and U.S. interests, directly and indirectly. Globally important critical infrastructure is vulnerable to cyber attacks and malicious cyber activity, placing military missions and economic systems at risk. Hostile actors engage in espionage in cyberspace by stealing defense-related intellectual property and trade secrets.

Some nations target U.S. partners with the intent to attack networks and to manipulate command and control and logistics data, which could adversely affect the U.S. military's ability to mobilize its forces in the event of a contingency, and then could amplify the effects through propaganda and information control. They also steal information unrelated to national security, such as proprietary economic and commercial information, which is then provided to competing companies in their countries.

The Department of Defense (DoD) is developing cyber forces to ensure and enhance military capabilities in all domains, provide cyber options for the President, and to defend the nation against cyber attacks and cyber adversaries.

## Policies, Oversight, and Relationships

*Policy & Doctrine:* Since establishing U.S. Cyber Command (USCYBERCOM) in 2010, the Department has developed policy and doctrine to determine how to operate in cyberspace, including Joint Publication 3-12, "Cyberspace Operations," and the 2011 Department of Defense Strategy for Operating in Cyberspace (DSOC).

In 2012, the Secretary of Defense approved the Cyber Mission Force (CMF) concept, dedicating resources to establish cyber teams in support of defending DoD networks, degrading adversary cyber capabilities, and supporting defense of national critical infrastructure. Since then, the Department has developed the "Cyber Force Concept of Operations and Employment" (CFCOE), a comprehensive, evolving, document defining CMF teams' roles, functions, and operational processes. The knowledge, skills, and abilities required for each cyber mission force work role (i.e., position) were defined in the "Joint Cyberspace Training and Certification Standards" (JCT&CS). The ability to assess individual and team readiness using a common set of joint tasks, conditions, and standards for all cyber mission team positions were defined in the "Cyber Mission Force Joint Training and Readiness Manual" (T&R Manual). To improve the quality, sufficiency, and efficiency of training, the Cyber Training Advisory Council (CyTAC) was established. Tri-chaired by representatives from USCYBERCOM, the Office of the Under Secretary of Defense for Personnel and Readiness (OUSD(P&R)), and the DoD Chief Information Officer (CIO), and in coordination with the Military Departments/Services, the CyTAC identifies, reviews, and assesses training requirements and standards for evaluation. It also addresses gaps between current and future cyberspace training capabilities. In addition, the DoD Enterprise Cyber Range Environment (DECRE) is a governance structure construct that

synchronizes efforts to promote effective and efficient utilization of security, operationally realistic and technical representative replications of the cyberspace domain.

In response to Section 932 of the National Defense Authorization Act (NDSS) for Fiscal Year 2014, the Secretary of Defense designated the Assistant Secretary of Defense for Global Strategic Affairs as the principal cyber advisor (PCA). In coordination with the Chairman of the Joint Chiefs of Staff (CJCS), the Combatant Commanders, and USCYBERCOM, the PCA will serve as the principal advisor to the Secretary on policies related to the CMF. In response to the Fiscal Year 2011 NDAA, Section 933, the Department established the Cyber Investment Management Board to facilitate alignment of Department cyber activities across science and technology (S&T), requirements, acquisition, development, test and evaluation (T&E), and sustainment. As an advisory board to key senior level Department decision-making bodies, the CIMB serves to ensure cyber investments are effectively planned, executed, and coordinated across the Department. The CIMB has met twelve times since its inception and has provided senior DoD leaders with an in-depth understanding of the Department's existing requiremetns baseline and current and planned investments in capabilities for cyberspace operations. To inform this process further, the Department recently established the DoD Cyber Operational Capabilities Board (COCB) to provide Combatant Commanders a forum to inject operational requirements into the acquisition process.

*Federal Cybersecurity Partnerships:* DoD is one component of the Federal cybersecurity team that addresses cyber threats to the United States. The Federal cybersecurity team includes:

- *Department of Homeland Security (DHS):* protects against, mitigates, investigates, and recovers from domestic cybersecurity incidents;
- *Department of Justice (DoJ):* investigates, attributes, disrupts, and prosecutes cybercrimes and domestic national security incidents; and
- *Department of Defense (DoD):* defends the nation from attack, secures national security and military systems, and protects information on Defense Industrial Base (DIB) systems.

*State-Federal Partnerships:* The Council of Governors (CoG), a bipartisan body of ten governors, was established by the President in 2010 for the purpose of further strengthening the partnership between the Federal and State governments to protect the United States and its people and property. The CoG exchanges views, information, and provides advice to the Secretary of Defense, Secretary of Homeland Security, and other senior Federal officials on matters regarding the National Guard, homeland defense, civil support, and synchronization and integration of State and Federal military activities within the United States. In February 2013, the CoG, on behalf of State Governors, and the Department approved the "State-Federal Consultative Process for Programming and Budgetary Proposals Affecting the National Guard," which established a sustained process to meet, confer, and exchange views and information in advance of the DoD determining programming and budgetary requirement priorities. This Consultative Process provides ways for Governors, through the Council of Governors and the Chief of the National Guard Bureau, to provide the States' assessments and requirements to DoD. The process also enables DoD to understand States' requirements more fully and to include these requirements for consideration in DoD's Planning, Programming, Budgeting, and

Execution process. In July 2014, the CoG, DHS, and DoD approved the "Joint Action Plan for State-Federal Unity of Effort on Cybersecurity." This Joint Action Plan is a commitment by the States, DHS, and DoD to work together to improve the nation's cybersecurity posture. It establishes a framework to guide State-Federal discussions in areas such as information sharing, operational coordination, and incident response. Similarly, the National Guard (NG) continues to play an important role bridging the gap between State and Federal governments as an established and trusted ally of both communities.

The strength of the NG derives from its roots in local communities. National Guard personnel are often community leaders who have direct connections with local industries and government officials and serve as the face of the DoD to our citizens. They are trusted members of communities who put on the uniform in times of natural disaster, as well as answering the call to duty for wartime missions. These community ties contribute to DoD integrating best practices from the business, public, and private sectors into defense training and operations, and through its cybersecurity partnerships, Federal training, and operations. Integration of the National Guard is a critical enabler that has allowed the U.S. Government to ensure our Nation can rapidly respond to any threat, foreign or domestic, and achieve the goals set forth by our Federal and State leaders. The National Guard's community presence and engagement of National Guard members in their civilian capacities in public and private sector organizations that are critical to continuity of operations at all levels of government and key private sector organizations make the National Guard uniquely able to contribute to a "whole of Government" and "whole of Nation" approach to securing U.S. cyberspace.

*Allies and Partners:* As directed by the President's International Strategy for Cyberspace in 2011, the Department works with allies and partners to expand situational awareness and shared warning systems, enhance cooperation in times of peace and crisis, and enable self-defense in cyberspace. Such partnerships bolster collective deterrence capabilities and strengthen the ability to defend the United States against cyber actors.

*Private Sector Partnerships*: The Department relies on the private sector to protect sensitive data related to DoD military operations across all domains (i.e., air, land, sea, space, and cyberspace). In collaboration with DHS, DoD fosters mutually beneficial partnerships with Defense Industrial Base companies through the DIB Cyber Security / Information Assurance (CS/IA) Program. This voluntary program helps protect DoD information residing on, or passing through, DIB company systems by facilitating information sharing between participating companies and DoD, as well as among fellow participants. As an optional component to the DIB CS/IA program, DoD developed the DIB Enhanced Cybersecurity Services (ECS), which furnishes classified cyber threat and technical information either to a DIB company or to the company's commercial service provider to counter malicious cyber activity in order to improve industry's ability to protect sensitive information related to DoD military operations.

## Cyber Missions

DoD needs the ability to maintain our advantage in cyberspace, and thus, across the other four domains, by conducting cyberspace operations and supporting military operations worldwide, supporting Combatant Commanders as they plan and execute military missions, and countering

cyber attacks and malicious cyber activity against the United States. Therefore, USCYBERCOM was created to centralize new and expanded cyberspace forces and capabilities under one command.

*U.S. Strategic Command (USSTRATCOM):* Defense against cyber threats requires the Department to strengthen its understanding of the complexities (capability and intent) of adversaries and risks to our systems to build resilience into our national critical infrastructure. The Unified Command Plan (UCP) assigns USSTRATCOM responsibility for synchronizing planning for cyberspace operations, in coordination with other combatant commands, the Services, and, as directed, other appropriate U.S. Government departments and agencies. These roles, however, have been delegated to its sub-unified command, USCYBERCOM.

*U.S. Cyber Command (USCYBERCOM):* USCYBERCOM has three primary missions. These missions are carried out, in part, by the Cyber Mission Force (CMF):

1. Secure, operate, and defend DoD networks;
2. Defend the Nation in cyberspace; and
3. Support Combatant Command (CCMD) full spectrum operations in cyberspace.

In December 2012, the Department approved a plan to establish a new cyber force resourced from all of the Services and NSA aligned to these three missions. Implementation of the approved CMF plan is underway with progress measured and reported on a quarterly basis.

*Cyber Mission Force:* The CMF is composed of three sets of forces aligned to achieve USCYBERCOM's three primary missions. Those sets are the Cyber National Mission Force, Cyber Combat Mission Force, and Cyber Protection Force. Once fully manned, trained, and equipped in FY 2018, these 133 teams comprising the CMF will execute the three primary missions with approximately 6,200 military and civilian personnel (see Figures 1, 2, and 3 in the classified annex).

> ***Cyber National Mission Force:*** The National Mission Force consists of 13 National Mission Teams (NMTs), supplemented by 8 National Support Teams (NSTs) (also called Direct Support Teams), which are designed to defend the Nation against strategic cyber attacks on U.S. interests. The NMTs are a counter-cyber force to stop cyber attacks and malicious cyber activity of significant consequence against the Nation.
>
> ***Combat Mission Force:*** The Combat Mission Force consists of 27 Combat Mission Teams (CMTs) focused on individual CCMDs requirements with the support of 17 Combat Support Teams (CSTs). The CMTs are designed to support CCMDs in carrying out approved operational plans and contingency operations with integrated cyber effects.
>
> ***Cyber Protection Force:*** The Cyber Protection Force consists of 68 Cyber Protection Teams (CPTs). The CPTs are further divided into four mission areas: National, DoD Information Networks (DoDIN), Combatant Command (CCMD) support, and Service support. All CPT units are focused on actions internal to the defended network, which primarily is within the DoDIN unless they are separately authorized to defend non-DoD networks. The core capabilities of these teams are mission protection, discover and

counter infiltration, cyber threat emulation, cyber readiness, and cyber support. These teams integrate and synchronize cybersecurity functions such as assessments of network vulnerabilities, penetration testing, remediation of vulnerabilities, and hunting on networks for adversary activity. CPTs will protect the most critical Service, CCMD, and national security networks (when authorized), as well as the Department of Defense Information Networks (DoDIN), supplementing their defenses. Additionally, CPTs will share malicious signatures and other indicators with interagency partners and appropriate critical infrastructure entities. There will be 18 national CPTs – six CPTs assigned to protect and defend the DoDIN, 24 CPTs for Service networks, and 20 CPTs for CCMD networks. The 18 national CPTs will work closely with the NMTs to understand specific adversary tactics, techniques, and procedures and capabilities to develop mitigation techniques (see Figure 2 in classified annex for detailed graphic).

## Operational Command & Control (C2)

In June 2013, the Secretary of Defense approved a new cyberspace C2 model. The Department selected the "Direct Support" model given the early stages of implementation of the CMF and continued maturation/integration of cyberspace expertise and planning at the CCMDs. Under this model, USCYBERCOM provides direct support to CCMDs through four Service-specific Joint Force Headquarters-Cyber (JFHQ-C). Implementation of the Direct Support C2 model is underway simultaneously as the CMF build continues (see classified annex for detailed description of the "Direct Support" C2 model).

## Resilience, Mission Assurance, and Continuity of Operations

To ensure resilience, mission assurance, and continuity of cyberspace operations, DoD is migrating the DoDIN to a more defensible network architecture, the Joint Information Environment (JIE). This architecture will maintain systems and capabilities that automatically and immediately failover to designed alternate capabilities, allowing operations to continue uninterrupted in degraded and denied environments. USCYBERCOM will lead the operation and defense of the JIE against attacks. As the JIE comes online, DoD is also taking steps to ensure that DoD asset owners and DIB partners meet the cybersecurity standards necessary to protect DoD's data and assure DoD missions.

DoD must defend its own networks against attack. As USCYBERCOM improves its force readiness, and the Services man, train, and equip the CMF (especially the Cyber Protection Teams) to joint standards, DoD must take steps to mitigate cyber risks and assure its most important missions are being met. To this end, DoD components will align their Cyber Protection Forces and other capabilities to prepare to defend their cyber key terrain, which is composed of networks and systems designated as mission-critical, Defense Critical Assets, and Task Critical Assets. Finally, DoD is working to strengthen the cyberspace aspects of its continuity of operations plans.

## Recruitment, Retention, Management, Equipping, and Training of the Force

The effectiveness of the CMF depends on the right people (military and civilian personnel) being recruited, trained, and then appropriately equipped to accomplish assigned missions. Overall,

DoD has made significant progress in adapting traditional recruiting, training, and retention methods for cyberspace-oriented military career fields. The Military Services use assessments, including the Armed Services Vocational Aptitude Battery (ASVAB), to determine individuals' aptitude for the cyber field. In addition, the Air Force, Navy, and Army are developing a joint computer-based "Cyber Test" to assess military applicants' propensity in a variety of computer and networking skillsets. The Services are also increasing their identification and recruitment of applicants with Science, Technology, Engineering, and Mathematics (STEM) backgrounds and working with their Service academies to identify and train potential cyberspace officers.

The Military Departments/Services' proposed plans (outlined in Section IV., "Way Forward") incorporating the Reserve Component (RC) into the cyber force, trained and certified to the same standards as active duty personnel, allows members of the military who wish to pursue civilian careers the opportunity to continue to serve their country. Although some Service members may receive higher pay in civilian cybersecurity jobs, the military cyberspace mission offers a distinct experience and unique opportunities for Service members to continue to serve in the RC as they train and execute military cyberspace missions not executed in the private sector. The RC provides an opportunity for members to continue to serve and leverage DoD's training investment to benefit both the private sector and DoD. Additionally, the RC provides an avenue for skilled civilian cyber personnel to enter the military, maintain their civilian job, and provide DoD with state of the art civilian knowledge.

Cyberspace forces need to be trained and equipped. The Joint Staff, USSTRATCOM, and USCYBERCOM have conducted several gap analyses to identify the capabilities required for cyberspace operations, and most recently, what the CMF teams need to conduct assigned missions. Additional requirements analysis is ongoing to identify requirements for next generation capabilities for cyberspace operations. The Military Departments have begun to equip these teams to USCYBERCOM joint cyberspace standards. USCYBERCOM's CMF Quarterly Readiness Report tracks the progress that the CMF has made toward equipping the Force. Specifically, it tracks network access and equipment status of all hardware, software, target access, and infrastructure resources required by CMF units.

USCYBERCOM is also working to decrease its reliance on the Intelligence Community (IC) infrastructure built to support foreign intelligence missions and develop independent access to global networks to conduct military operations. This infrastructure has different attributes than those required by the Intelligence Community, including the ability to scale rapidly, be disposable, cause minimal collateral damage to other capabilities if discovered by adversaries, and consistent with other warfighting domains, enable attribution of certain cyberspace capabilities and effects to the United States to deter adversaries from future aggression as required. Most importantly, this infrastructure will be available to the CMF to carry out its military operations against military-relevant targets. Access to independent infrastructure is not only important from a readiness perspective; it also prevents military actions from inadvertently exposing IC missions.

DoD's ability to maintain continuity and accomplish its mission has historically required a Total Force comprising of military and civilian personnel. Although the immediate, short-term effort to start and gain momentum building the CMF focuses on manning, training, and equipping

military personnel (active and reserve components), the Department is keenly aware of the need for a long-term strategy to integrate its existing and future civilian workforce into a cohesive Total Force construct. As discussed in Section IV., "Way Forward," deliberate actions are planned to examine the feasibility and options for various incentives to recruit and retain the best qualified civilian workforce. The results of those analyses will be integrated into the force structure as data becomes available.

*USCYBERCOM Training Standards:* The CMF method of employment directly informs the training criteria and standards established for individual team members and unit requirements. USCYBERCOM, in coordination with the Joint Staff, the Combatant Commands, the Military Departments/Services, and the National Security Agency (NSA), established joint training standards. These standards for individual and collective training are captured in the Joint Cyberspace Training and Certification Standard (JCT&CS), the CMF Individual Training Pipeline (ITP), and the CMF Training and Readiness (T&R) Manual.

The JCT&CS is based on the National Initiative for Cybersecurity Education (NICE) framework and is currently being updated, identifies the knowledge, skills, and abilities (KSA) required for each role on a CMF team. The JCT&CS is also designed to assist in shaping other DoD workforce initiatives such as the future DoD Cyberspace Workforce Framework.

The ITP identifies each individual's path to acquire the specific skills needed to satisfy the required JCT&CS standards. The development of these skills will assist the Services with identifying common joint training standards and solutions for other Service personnel working in the cyber domain.

The CMF T&R Manual provides tasks, conditions, and standards required to demonstrate individual and collective proficiency for CMF teams. Services, in coordination with its Service Components will supplement the standards with Service-specific requirements in order to exercise the collective capabilities of its cyber personnel.

USCYBERCOM is currently assisting the Service Components in meeting the joint training standards to accelerate the CMF build. The USCYBERCOM Individual Training Equivalency Board (ITEB) was developed in August 2013 to allow evaluation of awareness of suitable training that meets the skills required to perform CMF missions. The ITEB process provides the Service Components an opportunity to accelerate the development of personnel who are currently providing operational support to USCYBERCOM. It can also be used as a model for the Military Departments/Services and other DoD Components to identify personnel within the cyberspace community who have prior experience and training that may be applied to specific cyberspace positions in the CMF or supporting positions at joint force headquarters elements or combatant commands described in the Direct Support C2 construct.

The following highlights progress made by each Military Department/Service in developing a trained and equipped cyberspace workforce composed of military and civilian personnel. The Services' current and planned ways forward include integration of reserve forces to augment active-duty personnel and provide surge capacity to USCYBERCOM for emergencies and crisis actions. Progress made regarding active-duty forces is explained first and is followed by discussion of Reserve Component (including National Guard) alignment.

*Army Active Duty Progress:* In the past year, the Army has made tremendous progress in the recruitment, retention, management, and training of their Active Force personnel. The creation of a Cyber Protection Brigade and a new Military Occupational Series to identify the elite group of cyber personnel are just two indications of the fundamental transformations taking place.

As part of these changes, the Army is evaluating existing and proposed personnel policies to ensure that it has the necessary tools to recruit, educate, train, retain, and lifecycle manage its cyber force. The Army's accession efforts, aimed at attracting world-class cyber talent, are being informed by the Army's experiences with the Special Forces in terms of eligibility and suitability. The Army has started to implement a plan to identify personnel with the requisite cyberspace aptitude. The Army is also leveraging the Army Cyber Assessment to measure the technical skills of current soldiers who are candidates for the CPTs.

An Army CPT recruiting website is in development to market interesting and unique CPT opportunities to skilled candidates. The Army has also expanded its targeting of applicants with STEM degrees to improve production of officers with the needed technical skills. For example, the Army is working with the U.S. Military Academy (USMA) to identify past graduates whose field of study indicates that they may be candidates for entry into the cyber field. The Army is also working with U.S. Army Cadet Command to interview potential cyber candidates at 2014 Reserve Officer Training Corps (ROTC) summer camp. For the long term, the Army's Training and Doctrine Command (TRADOC) is developing an enduring program to standardize the recruitment, development, and training of USMA and ROTC STEM candidates.

The Army is also carefully assessing its training requirements. In accordance with the USCYBERCOM CMF implementation plan, the Army is following a phased build-out of its CMF teams. The Army derives individual CMF training requirements through the Joint Cyberspace Training & Certification Standards (JCT&CS) and the USCYBERCOM Joint Force Development training pipeline. To streamline training timelines for CMF personnel, the Army has maximized the reuse of the USCYBERCOM Individual Training Equivalency Board (ITEB) to waive specific required training requirements based on prior training and experience. Further, the Army is aggressively posturing to assume CMF individual training responsibilities from USCYBERCOM starting in FY 2017, and has modified its course offerings to meet USCYBERCOM standards. Ultimately, this streamlining effort will reduce the training burden on the Army to fulfill its CMF training requirements, while accelerating the operational readiness of CMF personnel. The Army's Cyber Center of Excellence (CoE) is undergoing a process to modify curriculum to meet USCYBERCOM requirements and reduce redundancy with Service requirements. For example, to be designated as an Army Cryptologic Network Warfare Specialist, a soldier must pass the 24-week, USCYBERCOM-approved, Joint Cyber Analysis Course (JCAC). The CoE has modified the requirements for the Army's Cyberspace Defense Technician to meet USCYBERCOM standards. In a similar effort, the CoE is currently modifying the Network Defense Specialist curriculum, and is conducting two pilot courses for this new Army Military Occupational Specialty (MOS). Army Cyber Command (ARCYBER) is developing a Cyber Training and Exercise Program that will leverage Combatant Command and Network Command exercises to address the Army's collective training requirements aligned to USCYBERCOM's joint standards where appropriate.

With all of these changes, the Army recognized potential personnel management efficiencies to be gained through the consolidation and management of its cyber population under one career field. The Army's Training and Doctrine Command is developing a cyber career management field, the 17-Series, which is currently projected for establishment by October 2015, if approved. Until the 17-series is approved, the Army Human Resources Command (HRC) will provide career management of cyber personnel through the recently established Cyber Electromagnetic (CEM) branch. HRC's CEM branch will provide appropriate career management to CMF-assigned personnel ensuring the Army's highly skilled talent remains within Army's cyberspace operations workforce for an amount of time commensurate with the Army's investment in them.

To facilitate HRC CEM's cyber talent management efforts, the Army recently established the E4, a new Additional Skill Identifier (ASI) based on skills, experience, assigned role, and unit of assignment that all CMF soldiers will receive. The objective of HRC's CEM branch is to provide interim career management for cyber-related MOS and functional areas for all Army cyber personnel identified for possible 17-Series conversion. The Army is preparing a separate officer skill identifier for cyber expertise or training received prior to commissioning and creating a retention plan for soldiers with this identifier.

To ensure that the Army continues utilizing the training and skills of its cyberspace workforce, soldiers serving on CMF teams will rotate to other CMF teams or other cyber units upon completion of their assignments. The E4 ASI designation will enable the Army to identify and track these skilled and experienced soldiers, and assignments to non-cyber units will be done only with the approval of the Commander of ARCYBER.

Civilians provide valuable skills and continuity to the cyber workforce, and the Army is actively recruiting and retaining skilled civilians. The Army distributes marketing materials to organizations with high densities of skilled candidates and employs a strategic communications effort to market the Army's efforts on the CMF to relevant publications. The Army seeks to hire skilled civilians from the ranks of former military personnel, colleges, and the private sector. The Army offers its current civilians professional development opportunities through existing NSA and Office of Personnel Management/National Science Foundation (OPM/NSF) programs such as NSA's Advanced Studies Program, OPM/NSF's Cybercorps Scholarship for Service Program, and NSA's Centers of Academic Excellence accreditation program.

In addition to monetary incentives, the Army offers education programs to develop soldiers further and act as retention incentives. For example, the Army offers Training with Industry programs and civilian graduate education and inter-Service education programs such as study at the Air Force Institute of Technology and Naval Postgraduate School.

*Air Force Active Force Progress:* The Air Force has made steady progress transforming its forces to meet the cyber threat, including establishing Air Force Cyber Command (AFCYBER) in 2009 and developing comprehensive programs to address recruiting, retention, management, and training of its cyber forces. The Air Force places special emphasis on recruiting and preparing its future airmen for cyber careers through national advertising campaigns highlighting STEM requirements and supporting cyber training and education programs for high school and college students nationwide. For example, the Air Force Institute of Technology's Center for

Cyberspace Research hosts the Advanced Cyber Education summer program for ROTC cadets from all Services who are studying computer science, computer engineering, or electrical engineering.

Like other Services, the Air Force screens potential service members based on test scores and educational achievement. For officers, a combination of type of degree and Air Force Officer Qualification Test scores are used to qualify for the cyberspace career field.

Once service members are in the Air Force, training programs are designed to develop Total Force professionals from numerous career fields with core training, including courses such as: Undergraduate Cyberspace Training, Cyberspace Defense Operations, and Intermediate Network Warfare Training. The Air Force also has developed an Intelligence Cyber Analyst course to train digital network analysts. This analyst training is complemented by the 24-week, follow-on JCAC. Additionally, cyber personnel can attend joint cyberspace courses based upon positional requirements and work roles. Finally, graduate level cyber curriculum and continuing professional education classes are offered at the Air Force Institute of Technology.

The Air Force carefully manages cyberspace airmen to balance practical and educational experiences in their fields. In addition to their continuing professional cyberspace education to maintain and build their expertise, the Air Force seeks to provide both breadth and depth to their airmen. For example, certain specialties will serve consecutive operations tours in cyberspace positions at different locations building depth as they progress through their career. This experience is coupled with continuing professional cyberspace education to build cyberspace expertise. Active duty service commitments ensure a return on training investments.

The Air Force has several tools to promote retention of qualified cyberspace airmen. To address manpower shortfalls in specific specialty codes, the Air Force has increased the minimum enlistment period from four to six years and increased the ability of community managers to control careers of skilled cyber enlisted and officers by prolonging cyber assignments. Furthermore, selective reenlistment bonuses (SRBs) are one of the Air Force's most flexible and effective methods of retention. They provide monetary incentives to retain existing members in critical skills that have low retention or low manning, as well as entice airmen from less critical skills to retrain into critical career fields.

For Air Force civilians, there are a range of hiring authorities and incentives to attract cyberspace personnel, including the Communication and Information Palace Acquire program, a three-year internship for recent college graduates with an interest in cyberspace. The program includes cyber training and benefits such as eligibility for student loan repayment.

*Navy Active Duty Progress:* The Navy has made progress toward full integration of cyber into its workforce including developing innovative programs such as the Cyber Warfare Engineer (CWE) program. In response to USCYBERCOM requirements for cyber systems developers, software engineers, and Research & Development (R&D) engineers (collectively referred to as “tool developers”), this highly competitive program recruits and commissions qualified enlisted sailors and civilians who hold specific cyber-related degrees. After five years of service as a CWE, participants are encouraged to either transfer into the Navy Information Warfare or Information Professional communities, or transition to the civilian DoD workforce.

The Navy is also seeking to create civilian positions to provide longevity and continuity within the cyber tool development mission force.

The Chief of Naval Operations (CNO) has placed a high priority on aggressive implementation of plans to manage discrete cyber career fields and within the CMF. Like other Services, the Navy uses multiple methods to recruit qualified candidates to the Navy's cyber workforce, including the ASVAB and Cyber Test, which are used to identify cyber aptitude.

The two primary enlisted cyberspace occupational fields, Cryptologic Technician Networks (CTNs) and Information Systems Technicians (ITs) are considered highly skilled, technical ratings and require significant training prior to their initial operational assignments. The JCAC serves as the Navy's feeder training course for the CTN rating, and is the foundational cyber training for all CTNs, including those filling highly specialized roles. The 19-week Network and Telecommunications Architecture and Information Assurance Course serves as the Navy's feeder training for the IT rating. A subset of IT personnel also attend the 18-week System Administration course. Additionally, all ITs are required to meet DoD Information Assurance certification requirements for privileged users.

CTNs and ITs have opportunities for advanced education at the Naval Postgraduate School, which offers a Master of Science in Applied Cyber Operations open to all Services. The Navy graduates of this program receive a specialty code and are detailed to select billets, including an opportunity to serve in the CMF. Navy increasingly offers cyber education opportunities to its officer corps, including mandatory cyber classes for Naval Academy Midshipmen. Starting in 2016, the Naval Academy will offer a Cyber Operations major. NROTC annually offers five "Cyber Option" scholarships to students that place highly in cyber. In addition to adding cyber areas of specialization to existing majors, such as Electrical Engineering, the Naval Postgraduate School (NPS) has developed the Network Operations and Technology program to understand more fully what is required to fight wars in the modern networked environment. NPS also offers a course to prepare officers to deploy cyber assets appropriately in the DoD cyber infrastructure. Furthermore, officers are able to obtain a Master's degree in cyberspace operations through the Navy's Information Dominance Cyber Program at Rensselaer Polytechnic Institute.

Based on the Navy's need to have a sustainable pool of personnel to support both Joint and Fleet requirements, enlisted and officer community managers monitor and adjust the number of personnel in each cyber rating. As requirements are identified in a rating, community managers fill them using a variety of methods including through recruiting, lateral transfers or conversions from other specialties, or commissioning qualified enlisted personnel into cyber-related officer designators. The Cyber Warrant Officer program is another important means of identifying, developing, and commissioning technically proficient sailors to contribute to and direct on-net cyber operations.

The Navy recruits and maintains a sufficient number of cyber personnel and ensures appropriate distribution across pay grades. Community managers and technical advisors provide recommendations for accession quotas each fiscal year, review requests for low-density/high-demand, community management requests, and provide recommendations for advancement quotas. The IT and CTN ratings use the standard Navy advancement quota management process for pay grade advancement. The ECM for each rating measures rating requirements and sets

quotas before each promotion cycle. CTNs and ITs have traditionally been very competitive ratings for promotion, allowing the Navy to promote very talented professionals. Similarly, officer community managers conduct community health assessments aligning billets, personnel, authorizations, and promotions. They also work with officer detailers to ensure officer promotion paths and community-valued billets guide officer assignments.

To retain qualified cyber sailors, the Navy uses monetary incentives, bonuses, and promotions. Qualified CTNs may be eligible for automatic advancement to the grade of E4 with a six-year enlistment contract as a part of the Advanced Technical Rate Program.. The Navy also offers significant retention bonuses for qualified CTNs. Rating conversion bonuses are also available for qualified sailors.

*Marine Corps Active Duty Progress:* As the smallest Service with a still growing cyber requirement, the Marine Corps has placed careful attention on ensuring that it meets its recruiting goals, particularly in the cyberspace workforce. The Marine Corps uses existing recruiting and retention tools to grow and maintain cyberspace operations forces and continues to meet its recruiting targets. As an initial assessment, the Marine Corps uses the ASVAB to screen qualified personnel for all entry-level occupations and every MOS. However, the more highly skilled occupations, such as cyber operations, are not considered entry-level professions and are sourced by moving qualified candidates from other feeder occupations.

In an effort to attract the most qualified Marines, the Marine Corps has expanded the feeder occupations to increase the pool of available candidates while also focusing on Marines whose current skills translate well into cyberspace operations. Additionally, incentive pay remains critical to this effort. SRBs allow the Marine Corps to shape the career force by targeting critical cyber MOSs and supporting lateral movement of Marines into them.

To train the Marine Corps' cyberspace workforce, the Marine Corps uses a combination of Marine, Joint, other DoD, and other Service schools. Two specific programs of study currently in place for the Marine Corps cyber security personnel are the Information Assurance Scholarship Program (IASP) and the Northern Virginia Community College Advanced Standing Initiative (NVCC ASI). The IASP provides the Marine Corps the ability to develop a skilled cyber security workforce through participation in a graduate education program. The program has placed more than 600 graduates into Cyber Security/Information Assurance positions DoD-wide. The NVCC ASI allows the Marine Corps to transfer 22 Marine Corps formal school courses into college credits toward an Associate in Applied Science (AAS) in cyber security degree from NVCC. In addition, the partnership between the Marine Corps and NVCC takes advantage of the NVCC and University of Maryland 2+2 program, which allows all of the credits earned for the AAS degree to transfer to the University of Maryland toward a Bachelor of Science in cyber security. This program incentivizes Marine Corps personnel, trained in Marine Corps formal schools, to further their personal and professional education.

The Marine Corps manages its cyberspace operations workforce in the same manner as the rest of its workforce by utilizing the Marine Corps Total Force System to track training and specialized skills. This allows the Marine Corps visibility into manpower allocations across both the active and reserve components. The Marine Corps' promotion system ensures that all

eligible Marines receive full and equitable opportunity to compete for promotion against other Marines of the same MOS. The Marine Corps will continue to promote Marines to maintain the required end-strength in each grade and MOS, as well as identifying and providing guidance to promotion boards for critical MOSs requiring special consideration. If necessary, the Marine Corps has a variety of tools that can be employed to retain qualified Marines, including continuing education programs. In particular, the IASP described above is a longstanding retention tool that is available to all DoD Components.

The Services have been able to recruit, train, and retain their cyber Active Force well in order to meet USCYBERCOM's requirements. As the CMF comes online, these forces will continue to be equipped and have the appropriate infrastructure to fulfill CMF missions.

## III. Current Reserve and National Guard Units

### Manpower and RC Requirements

The Services are working closely with their Reserve Components to develop Total Force solutions to their cyber workforce plans, tailored to the responsibilities and requirements of each Service. The Services are collectively pursuing growth strategies that ensure the optimal force mix to deliver an effective and efficient Total Force solution to our nation's growing cyber threat. Each Service has developed Reserve Component integration strategies that embrace Active Component capabilities in the cyberspace domain, and leverages the Reserve and National Guard strengths from the private sector and corporate knowledge from a long-standing force in the cyber domain that is critical to our operations in all domains. These strategies will ensure that DoD embraces cyber expertise from all sources integrating diversity of thought, rapid innovation, and best practices. This mix of strengths from a Total Force approach is essential to keep DoD in the forefront of innovation. This approach ensures the availability of cyber capabilities on the global stage as well as for defense of the homeland, where National Guard and Reserve forces reside.

*Army Reserve Components:* The Army Reserve Components are the U.S. Army Reserve (USAR) and the Army National Guard (ARNG). The USAR is generally aligned into unit structures but does have some individual augmentees throughout the cyber portfolio. Today, the Army's RC supports Army cyberspace operations with a variety of skills and units, using soldiers with civilian acquired skills to fill critical positions, mostly in the classic Computer Network Defense-Service Provider (CNDSP) role. The USAR currently has approximately 620 cyber positions across its force structure that conduct Defensive Cyberspace Operations (DCO) and DoDIN operations on computer networks and systems operated by DoD, including vulnerability assessments, forensic analysis, information assurance, and incident handling. The RC provides direct support to USCYBERCOM, the National Security Agency, and Defense Information Systems Agency (DISA) for planning and collective training, intelligence targeting and protection, and defense of applications of the DoDIN, thereby ensuring its availability and survivability.

*USAR:* The Information Operations Command (ARIOC) is authorized 308 billets, and functions as the center of all support to cyber capabilities in the USAR. It has five battalions stationed across the country, and conducts CNDSP missions in support of Army networks and provides DoDIN operations and CNDSP support to the Southwest Asia Cyber Center. DISA and USCYBERCOM missions are augmented by support from individuals assigned to USAR at DISA and USCYBERCOM Army Reserve elements.

*The ARNG* has authorizations for personnel with cyber expertise that varies depending on their position. They provide operational support, including through Joint Force Headquarters Computer Network Defense Teams (CND-T), and ensure critical cyber capabilities are available to support civil authorities. Many States increased CND-T slots beyond the authorized 8 in anticipation of the Cyber Force build up.

The Virginia ARNG Data Processing Unit (VA DPU), conducts full-spectrum cyber operations in support of USCYBERCOM and others when activated. An associated eight-person Information Operations Support Command (IOSC) provides ARCYBER with C2 support.

The bulk of the ARNG's cyber capabilities are found in 54 standing CND-Ts and Joint Force Headquarters-Directorates of Information Management (JFHQ-DOIM) located in the 54States, territories, and the District of Columbia. Authorized eight positions per team, they conduct DCO and information assurance missions to protect the ARNG networks in each of the States and territories where they interface with the DoDIN.

As the Army implements its plans for a Total Force approach to cyberspace operations, it will continue to assess and analyze missions and manpower to refine those requirements for both the Active and Reserve Components.

*Air Force Reserve Component:* The Air Force Reserve Components are the U.S. Air Force Reserve (USAFR) and the Air National Guard (ANG).

*The USAFR* supports Department cyber missions across the gamut of cyber skillsets, utilizing all statuses in both full- and part-time alignments. The USAFR presents forces by leveraging both the Classic Associate unit construct and individual mobilization augmentees (IMAs). The entirety of the USAFR cyber portfolio, including support operations at Air Force bases, currently totals 3,853 military personnel and is aligned to support Air Force Cyber Command (AFCYBER) in its CNDSP role across every CCMD and major command. To do this, the Air Force uses IMAs, traditional reservists, air reserve technicians, active-duty, and Active Guard Reserve personnel. Additionally, 223 civilian positions throughout the reserve portfolio provide steady-state continuity of cyber operations.

Direct cyber capabilities conducting DCO and DoDIN Operations support are consolidated within the reserve 960$^{th}$ Cyber Operations Group (960$^{th}$ CyOG) located at Lackland Air Force Base in Texas. The 960$^{th}$ CyOG provides capabilities to AFCYBER, including operational-level cyber command and control, network and vulnerability management, defense analysis, and network extension.

The 960th CyOG currently has 140 full-time and 752 part-time positions, as well as eight squadrons and two flights spread across the United States, including four combat communications squadrons. The 960th CyOG's 378 combat communications personnel build and maintain communications networks and physical cybersecurity infrastructure for DoD. Its four squadrons are located in California, Georgia, New Jersey, and Oklahoma (an inventory of the 960th CyOG facilities and equipment is in Annex 1).

*The ANG* has 590 personnel who serve in eight States and provide full-spectrum cyberspace operations support through nine units organized into four Network Warfare Squadrons (NWS), four Information Operation Squadrons (IOS), and one Information Aggressor Squadron (IAS). Although some of these units are organizationally aligned to the CNDSP role, they are also available to their respective Governors when not performing their DoD functions (an inventory of ANG squadrons and equipment is in Annex 1).

Additionally the ANG has five cyber Intelligence, Surveillance, and Reconnaissance (ISR) units with 435 total personnel in three States aligned under the Active Component's 659th ISR Group. The ANG ISR cyber units, 218th ISR Group (Tennessee), 223rd Intelligence Flight (Kentucky), 124nd Intelligence Squadron (Ohio), and 256th Intelligence Squadron (Washington), and a Maryland ANG squadron yet to be determined, are air components of the Director of National Intelligence.

*Navy Reserve:* Unlike the Army and the Air Force, the Navy has no dedicated cyber Reserve unit based structure; for the most part, individual reserve cyber personnel augment Active Component teams or provide overall mission support. Current reserve personnel augment headquarters functions on the cyber plans and targeting and fires efforts and one reserve unit supports the headquarters functions of USCYBERCOM. Navy Reservists also fill significant and varied roles in FLEET CYBER COMMAND/COMMANDER 10th FLEET (FCC/C10F) efforts to build and deploy its CMF structure. FCC/C10F's Reserve personnel develop strategic planning for CMF team-specific concepts of operations, and plan and formalize the design for the Active Component's Navy CMF team build, which is currently under review by FCC/C10F. In addition, reserve personnel continue to work with the active component to develop a coherent reserve strategy to support the CMF. Navy Reserve elements are working with their active counterparts to provide a roadmap to integrate reserve cyber assets into the Active Component's CMF missions from FY 2015-FY 2018. A small number of reservists are assigned to support the Navy Joint Force HQ-Cyber element as IMAs.

The Navy is conducting ongoing mission analysis to develop a Total Force implementation strategy outlining the alignment of reserve cyber-coded billets. This will allow the Reserves to support the full spectrum of the Navy's cyber mission areas, including the administration, command and control, training, and operations of its cyber mission forces. In addition, FCC/C10F is conducting a review of all RC forces assigned to the Commander 10th Fleet (C10F) based on skill set and work role to determine who should fill the Navy-sourced CMF teams.

The Navy resources its cyber domain requirements from the Information Dominance Corps (IDC) composed primarily of Information Warfare and Cryptology personnel. Intelligence and Information Professional personnel are also added as needed. Of the approximately 6,700 IDC

reserve personnel, more than 1,500 are dedicated to supporting C10F, the NSA, and the National Reconnaissance Office (NRO). These 1,500 are divided between 34 Reserve Component units. Navy reservists currently support Active Component cyber exercises and can provide immediate, trained, and experienced operators to augment the active force when needed.

Navy Reserve Forces has realigned 305 FY 2015-FY 2018 billets to enhance support of cyber missions. These personnel will align across the 34 dedicated units and, in addition to supporting C10F, NSA, and NRO, will be accessible for cyber missions to USCYBERCOM as required.

*Marine Corps Reserve:* The Marine Corps Reserve cyberspace operations workforce consists of traditional Selected Marine Corps Reserve and IMA detachments currently augmenting Marine Forces Cyberspace Command. The vast majority of these personnel are cyber network operations personnel within traditional communications elements, as well as a small number of cyber security technicians and signals intelligence analysts.

The Marine Corps uses its reserve forces to augment Active Component needs and ensure the best resourcing of Marine Corps requirements. With the exception of a dedicated IMA detachment at Marine Forces Cyber headquarters, the Marine Corps does not initially intend to use the Reserves to fill CMF requirements. Currently, reserve support for all cyber requirements will be focused on areas within cyberspace that are less time sensitive than the anticipated requirements of the CMF. Although the Marine Corps does not intend to use reserve personnel for the CMF build at this time, it recognizes the criticality of this mission and understands that this is an area of evolving needs that will require continuing study and evaluation.

## Recruitment, Retention and Career Paths for Skilled Reserve Component Personnel

*Army Reserve Components:* The Army's objective is to ensure that its Total Force has the necessary tools at each stage to recruit, educate, train, retain, and manage a first rate cyber force. The USAR and ARNG are well-positioned to allow skilled individuals to continue serving their country while pursuing civilian job opportunities. Talented individuals are encouraged to join the USAR or the ARNG to conduct cyber activities which are sanctioned only through military authorities. Talented individuals are also eligible for a progressive grade structure that allows soldiers to achieve an accelerated military career progression. Soldiers with critical skills who plan to leave the Active Component are encouraged to affiliate with the RC through incentive programs, such as student loan repayment programs. Partnerships with private and public organizations also provide a valued source of skilled Service members.

The Army HRC provides centralized personnel management for all USAR soldiers in accordance with Army regulations and is responsible for career management, sustainment, distribution, and transition of USAR personnel optimizing leader development, and for enabling readiness and a balanced and versatile force. The ARNG performs commensurate personnel management functions for ARNG soldiers with guidance from the National Guard Bureau. The RCs, like the Active Component, are subject to the creation of the provisional Army Cyber Branch in March 2014. Upon Headquarters' approval of the 17-Series concept, this provisional Cyber Branch will transition to provide career management for all USAR 17-Series soldiers. Similarly, the

National Guard Bureau (NGB) will determine the most appropriate method to manage ARNG 17-Series soldiers.

*Air Force Reserve Components:* The USAFR and ANG will continue to leverage existing accession tactics, particularly in proven recruitment areas such as the San Antonio region, where the majority of existing USAFR cyber resources are located. The USAFR and ANG will continue to employ selected cyber skill incentive programs, both for initial entry and retention, for those with highly competitive cyber skills.

The USAFR and ANG also focus heavily on retention of highly skilled personnel from the Active Component. This retention allows them to provide manpower at a lower overall training cost than the active component. Additionally, Reserve and Guard members are able to leverage their civilian experience and traditionally turn over at a lower rate leading to a significantly more robust experience base. Longevity in position gives depth to ANG forces, additionally, more experience for ANG personnel by leveraging military and civilian expertise and training. These strengths allow the Air Force and ANG to present a lower life-cycle cost for increased warfighting capacity and capability.

All components use annual performance reviews to identify and highlight top performing airmen, aligning these high performing officers and enlisted personnel toward command, joint, and key cyber positions. Specific career milestones are consistent across components to ensure that cyber airmen may move between cyber mission opportunities, regardless of component.

*Navy Reserve:* The Navy Reserve has multiple paths of entry into the cyber profession for both officers and enlisted personnel. This includes directly entering, laterally transferring, or converting into cyber specialties. Qualified enlisted members are also encouraged to apply to commissioning programs.

The Navy continues to take a holistic Total Force approach to building and maintaining its highly skilled cyber forces. The management of discrete, critical cyber career fields remains a high priority for the Chief of Naval Operations and the Navy using the IDC to manage its well established cyber career path, including its reserve cyber components. The IDC community managers will continue to ensure that the CTN and IT rates are properly aligned and integrated within the Navy's Total Force to support both the Joint and Fleet requirements for cyberspace operations.

*Marine Corps Reserves:* The Marine Corps is committed to treating the cyber skills as it does other skills in the Reserve Component and is working closely with force planners, trainers, and recruiters to tailor and target its recruitment of critical cyber skills to meet its cyber requirements.

## Skills and Training

In order to conduct DoD missions, RC personnel are required to meet the same training standards as Active Component (AC) personnel. USCYBERCOM currently provides the Services joint training for CMF personnel with the intent the Services will establish and implement long-term plans to train CMF personnel starting in FY 2017. However, each Service is responsible for

training its CNDSPs, which takes approximately 24--weeks. These Service members are then required to meet each Service's standard for specific cyber missions.

The CFCOE identifies all of the cyber roles and the associated KSAs an individual should possess to perform on a cyber mission team in each of the five basic team roles: Analyst, Enabler, Manager, Operator, and Planner. The KSAs are in the areas of Computer Science, Cryptology, Cyber Security, Network Exploitation, Technology Operations, Oversight and Compliance, Reporting, Information Research, Communications Intelligence Signals Analysis, and Analytic Tools. These KSAs apply to both AC and RC teams. Due to the experience and skills the Reserve Cyber Components often bring to the total force, DoD will use the existing ITEB to look for opportunities to gain efficiencies from experience outside the standard training models within the Services. The ITEB is a panel of subject-matter experts from USCYBERCOM, the NSA, and the Service Components who evaluate an individual's training, education, and experience (skill level) to determine if the individual should be granted relief from classes in the training pipeline, as identified in the CMF T&R Manual. This allows the Services to recruit, assign, and retain Reserve and National Guard personnel based on the same model used for AC personnel. USCYBERCOM's T&R Manual contains the individual, sub-element, and collective training requirements required for all CMF teams, regardless of whether a position is filled by AC, RC, or civilian personnel. This allows DoD to oversee a robust sustainment program that ensures continued proficiency and attrition offset to enable continuity of the Total Force and the ability to complete the mission.

*Army Reserve Component*: The Army RC contains personnel with varying levels of cyber skills. Both individual and team skills have been acquired through industry, academia, government and military training.

In the near-term, the Army is exploring options for training of RC personnel. Potential options include streamlining the training pipeline and course structure to fit more closely the consecutive Reserve Component Institutional Training model, and allocating sufficient funding and training resources to institute and sustain a robust training plan. The Army is posturing to assume CMF individual training responsibilities from USCYBERCOM no later than FY 2017 for both the Active and Reserve Components of the Army and is continuously working with USCYBERCOM to certify its cyber MOS schools. Contingent on the availability of resources and completion of the Active Component CMF build in FY 2017, RC CPT soldiers should begin training in an MOS required for CPT work roles (Cyber Network Defender, Information Protection, and Cryptologic Network Warfare) starting in FY 2017.

*Air Force Reserve Component:* RC and AC personnel receive the same training for the same mission sets. Just as active-duty cyber airmen attend undergraduate cyberspace training, Cyberspace Defense Operations Training, and Intermediate Network Warfare Training, so do Reserve and Guard counterparts. Although the Reserve and Guard are able to provide an Airman initial skills training and Network Warfare Training, the length of training is extensive. Capturing transitioning AC cyber skills is critical to Air Force Reserve and Air National Guard success. Since Air Force Reserve and Air National Guard personnel are embedded in all cyber missions, every transitional AC member will have existing skills that will be beneficial in the Air

Force Reserves and Air National Guard. Additionally, capturing civilian acquired skills in the Air Force Reserves and Air National Guard is critical as well.

The cyber mission skills are complex and leveraging the skills that part-time Airmen gain in their civilian capacity can be helpful to DoD. It is often the case that the skills required to defend civilian networks are similar to those required to defend the Air Force Network. Currently, cyber defensive skills are the most critical due to an extremely small number of AC Airmen transitioning to the Air Force Reserves due to the relatively new active career field and service commitments.

*Navy Reserve:* The Navy recently realigned 305 FY 2015- FY 2018 billets to support cyber missions. These billets will be phased in over the next four fiscal years, with approximately 13 percent established in each of the first three years and the remaining 60 percent in FY 2018. The Navy is conducting a mission analysis to determine how to employ these and other existing C10F RC forces most effectively across the Navy's assigned Joint and Fleet cyber mission areas. Throughout this billet review, Navy Reserve personnel continue to collaborate with USCYBERCOM, the Office of the Chief of Naval Operations (OPNAV), and FCC/C10F Active Component stakeholders to implement a holistic employment strategy and structure.

*Marine Corps Reserves:* The Marine Corps has standardized cyber training requirements that must be met by both AC and RC personnel. These standards are institutionalized in Marine Corps training and readiness manuals.

## Reserve Component Infrastructure

*Joint Infrastructure:* The Services' cyber forces have the ability to access, if needed, any of the 27 Joint Reserve Intelligence Centers (JRIC). The purpose of these sites has been to provide joint intelligence production and training activity that use information networks to link members of the RC with the Combatant Commands, Military Departments, and Combat Support Agencies (CSA) through joint intelligence production and training. Although the traditional focus of these sites has been to support the IC as a whole, the connectivity and capacity of the sites allow them to support the needs of the Reserve cyber force as well; an un-forecasted requirement, however, may affect current missions and stress existing capacity. As USCYBERCOM presence grows in the JRICS, their requirements will be included in site capacity and utilization considerations so as not to present unnecessary negative impacts on current missions or stress existing capacity.

The current JRIC structure consists of 27 sites, with more than 388,000 square feet of classified workspace connected through the IC's IT infrastructure. Individual JRICs are hosted by the Services and National Guard providing reciprocal access to sister services and other national level agencies. Presently more than 300 RC units, including National Guard assets, leverage JRICs (Service-specific Reserve Component infrastructure is in Annex 2).

Cyber Reserve Components may also have access to sensitive compartmented information facilities (SCIFs) sponsored by other organizations, primarily active-duty bases, providing an opportunity for RC members to integrate and collaborate regularly with their AC partners. Finally, the ANG has 51 accredited SCIFs and an additional 17 under construction. The ARNG has 37 accredited SCIFs.

## IV. Way Forward

In the near term, adequately manning, training, and equipping the CMF remains the Department's top cyber priority. There is a significant role for the RCs to support the Department's cyber missions. To provide that support most effectively, however, force structure and infrastructure should be developed in the RCs as requirements arise. The extent of the RC role in supporting future cyber missions is not yet determined, and will be better understood over time. As noted in the opening section of this report, the conclusions and way ahead articulated below represent the Department's informed assessment today. Cyberspace is a dynamic domain, and the Department's approach will adapt as this operational domain matures, our forces become operational, and the threat landscape evolves.

### CMF requirements that may be filled by the Reserve and Guard

The CMF workroles defined in the CFCOE do not articulate how the Services should fill CMF positions. The Services may elect to fill their CMF positions with AC or full-time equivalent RC personnel as long as those personnel are trained to USCYBERCOM joint standards as prescribed by Secretary of Defense guidance and joint standards, and equipped to the same standards to accomplish the mission. Although there are qualified RC personnel to perform NMT and CMT tasks, for the most part RC personnel align most closely with the CPT mission, which is the most similar to their professional civilian roles.

### Current RC support to USCYBERCOM Headquarters

The Services' RCs already provide Headquarters support to USCYBERCOM. Currently, USCYBERCOM has 74 reservists from each of the four Services providing part-time support to USCYBERCOM's J-series directorates through the Joint Cyber Reserve Element (JCRE). The personnel are a mix of IMAs and unit-based personnel. The Services retain responsibilities for manning, training, and equipping assigned members, while the JCRE facilitates mission tasking, exercise augmentation, and joint administrative duties.

### Services' RC plans for the CMF

In addition to filling limited Reserve billets at USCYBERCOM Headquarters, the Services are required to present forces for the 133 CMF teams. To fulfill their requirements, the Services propose to use their RC forces to fill or augment these teams. The Army, Navy, Air Force, and Marine Corps have several options for integrating their RC personnel into the CMF as potential future surge capacity.

In total, the Army's proposed plan would field one full-time ARNG CPT, and 10 part-time ARNG CPTs and 10 part-time USAR CPTs. These Army RC Forces would consist of additional ARNG personnel and USAR personnel above the Army's current CMF requirement to fill critical Service needs. The Air Force's proposed plan would field two CMF-required CPTs filled by 12 ANG squadrons, and the cyber operations portion of one CMF required NMT will be filled by three squadrons on a rotational basis and by the equivalent of one full-time CPT, distributed across three CMF-required CPTs, consisting of three Reserve units made up of 127 USAFR airmen. And lastly, IMAs from the Navy and Marine Corps to ensure that teams are

always fully manned. In sum, approximately 2,000 RC personnel, all trained and equipped to the same joint standard, would be available as CMF surge capacity.

There will be advantages to using RC resources for CMF missions, such as providing load sharing with active duty forces, providing available surge capacity if authorized to mobilize, and offering DoD trained forces to aid in the defense of national critical infrastructure if requested and authorized. Several factors should be considered when determining the CMF force structure and the mix within the Total Force. These factors include whether the position is military essential, deployment frequency and duration, speed of response, unit readiness for specific mission sets, and costs.

## The Army

The Army's proposal is pre-decisional and has not yet completed the Program and Budget Review cycle. Its proposed RC integration plan to provide 20 part-time CPTs and one full-time CPT will be over and above their current CMF requirement. The Army plans to train and equip all 21 teams to the same joint standard creating surge capacity to ARCYBER and USCYBERCOM.

*The Army National Guard:* ARNG CPTs would conduct defensive cyberspace operations for under-resourced cyber requirements, and if available, could support DoD Defense Support of Civil Authorities (DSCA) or homeland defense missions in Title 10 or Title 32 status, if authorized, and support other appropriate State missions determined by the Governor in State active duty status. The Army plans on creating ARNG structure with personnel resourced through Total Army Analysis 2016-2020. The ARNG's proposed part-time CPTs would likely be located at existing ARNG secure facilities. However the Army continues to assess available infrastructure and would identify final stationing locations that leverage earlier investments. Stationing decisions are expected to be finalized in FY 2015.

*The Army Reserve:* The Army plans to transition the 308 personnel in the Army Reserve Information Operations Command (ARIOC) to the Army Reserve Cyber Operations Group (ARCOG), which would consist of 469 personnel. The USAR would build 10 part-time CPTs to conduct defensive cyberspace operations for under-resourced cyber requirements, and would support the C2 structure associated with the USAR cyber force.

The USAR would locate future units at existing secure facilities and infrastructure in Adelphi, MD, Pittsburgh, PA, Devens, MA, Fort Sam Houston, TX, and Camp Parks, CA. Although the Army plans to leverage existing equipment and infrastructure to the maximum extent, some additional infrastructure may be required at select locations.

The Army's proposed establishment of 21 new RC teams and associated C2, intelligence, and training support will introduce new costs to the Army budget that are not yet resourced and have not yet been through the Program and Budget Review process. Therefore, these plans are subject to change. The Army assesses that there would be manpower, equipment and infrastructure, maintenance, travel and support, and training costs starting in FY 2017. The equipment costs primarily would be for each CPT to have its own deployable CPT kit, each estimated to cost $115K. The Army is currently developing these deployable tool kits for fielding to its CPTs.

These deployable tool kits enable on-site responses to cyber incidents. The Army is currently conducting financial analysis to determine the cost to man, train, and equip these CPTs and plans to request resources to support these costs in the future Program and Budget and Review cycles.

## The Air Force

The Air Force's proposed plan would use the USAFR and ANG to support steady-state and surge capacity for the CMF build. The plan calls for realigning approximately 600 ANG personnel to generate two full-time, CMF-required CPTs and the cyber operations component of one CMF-required NMT. Additionally, they will realign 127 USAFR personnel to fill one-third of three CPTs. This plan is contingent upon available resourcing through FY 2016.

*The Air National Guard:* The Air Force plans to use the ANG to staff two CPTs with leadership, operational, and maintenance support generated from 12 ANG squadrons. The 12 squadrons would rotate between active and dwell status to provide two continuous full-time CPTs to support USCYBERCOM's mission to defend DoD networks. These two continuous full-time CPTs would be generated from three existing NWS (the 261st NWS from California, the 143rd NWS from Washington, and the 262nd NWS from Washington); four repurposed units (the 132nd Communications Flight from Iowa and, one Maryland, one Pennsylvania, and one New Jersey ANG unit to be determined); and five units to be identified.

Additionally, the Air Force plans to use the ANG to generate the cyber operations component of one NMT co-located at NSA Washington. The cyber operations component of an NMT consists of 22 cyber operators and is organized as a Unit Type Code (UTC). The NMT UTC would be generated from three squadrons: the 166th NWS from Delaware; the 175th NWS from Maryland; and one Maryland ANG squadron yet to be identified.

In total, 12 part-time CPTs generated from 12 ANG squadrons and the cyber operations component of one NMT from three existing ANG squadrons provide a total of 15 ANG squadrons fulfilling two full-time CPTs and a portion of one full-time NMT as part of the Air Force CMF requirement. The ANG would contribute approximately 600 personnel to generate the two CPTs and the cyber operations component of the NMT. Some of these authorizations would be taken from other ANG missions to augment the cyber mission. These CPTs and the cyber operations component of the NMT would be trained to the same joint standard. The 10 teams in dwell status not being used for the CMF would be available as surge capacity.

*The Air Force Reserve:* The Air Force plans to use USAFR forces for three part-time CPTs. The three USAFR CPTs working in a Classic Associate Unit partnership provide equivalent capacity of approximately one full-time CPT. The USAFR would provide three UTCs for each of the five teams within a CPT. The construct is advantageous to the Air Force and USCYBERCOM because it creates a surge CPT capability, in addition to load-sharing the steady-state responsibility. If authorized to mobilize, this construct would allow the Air Force to build out three full-time CPTs to conduct around-the-clock operations.

In total, the USAFR would have 39 full-time positions, consisting of eight Active Guard Reserve Officers and 31 Active Guard Reserve Enlisted personnel, and 88 part-time positions, consisting of 13 Traditional Reserve Officers and 77 Traditional Reserve enlisted personnel. These 127

reservists would fill positions with qualified personnel currently serving in cyber positions. However, the USAFR would not re-mission any squadron to meet the demand. In addition to the CPT plan, the USAFR plans to provide 15 IMA positions in FY 2016 to 24th Air Force for use in its role as JFHQ-C Texas.

The Air Force's proposed plan to establish these CMF and surge teams would introduce new costs to the Air Force budget that are not yet resourced. Though not yet approved, the Air Force submitted a request for funding in its FY 2016 Program and Budget Review Cycles. The equipment cost primarily would be for each of the 12 ANG units and the two active-duty CPTs to buy and sustain their own Cyber Vulnerability Assessment (CVA) system to conduct their hunt missions. The three part-time USAFR CPTs would use the AC's CVA system and, therefore, would not have an initial equipping cost.

### The Navy and Marine Corps

The Navy is working to provide a seamless integration of RC assets in support of AC cyber mission requirements. Fleet Cyber Command has determined that there is not currently a need to establish cyber units as a part of its reserve component units, but will develop individual billets to support cyberspace operations headquarters units as needed. The Navy realigned 305 Reserve billets for FY 2015-FY 2018 to support cyber missions.

Similarly, the Marine Corps will use, wherever possible, individual billets within its individual augmentation units to support cyberspace operations headquarters units as needed. Since the immediate use of reserve personnel for the CMF is not intended, the Marine Corps will therefore continue to study and evaluate the potential use of Reserves for this mission.

The plan to leverage reservists as augmentees when necessary will help ensure that the Navy and Marine Corps teams are always fully manned. Therefore, these personnel will be trained to the same joint standard. Although minimal training resources will be necessary, there is no expected cost in the next two fiscal years for either plan. Once a final cost concept is approved as part of Reserve Force integration strategies, final training requirements will be defined and funding requested. Funding is not associated with initial skills training, but instead will be specific to operational training required to perform augmentation duties.

## V. Department's Assessment

DoD is in the early stages of developing the CMF, and the Services' proposed plans for RC integration are subject to significant changes as the CMF evolves to meet the cyber threat environment. Today, the Department's assessment is that the CMF model and size are appropriate to address the current threat. However, when the CMF was established and approved, it did not account for surge capacity or for unique missions outside the scope of those the CMF is responsible for conducting. Therefore, although it will require additional evaluation and study, it is DoD's assessment that additional capability may be needed for both surge capacity for the CMF and to provide unique and specialized capabilities that can contribute to a "Whole-of-Government" and "Whole-of-Nation" approach to securing U.S. cyberspace.

Many factors go into the force development and force mix, and, therefore, it is too early to prescribe the appropriate mix. In the near-term, however, the Department assesses that the Services' proposed plans are a good first start, and those plans will be reevaluated on a periodic basis.

## Assessment

The Office of the Secretary of Defense (OSD) conducted a number of consultations with key stakeholders to ensure a transparent process and provide a comprehensive analysis. OSD Cyber Policy solicited input from the Reserve Force Policy Board, State Adjutants Generals, the National Guard Bureau, the Guard Senior Leadership Council, the Department of Homeland Security (DHS), and the States, through the Council of Governors. Through these engagements, the Services, OSD, the Joint Staff, the National Guard Bureau, USCYBERCOM, DHS, and the States provided the data and analysis that form the backbone of this report. This report reflects the Department's current view, and is expected to change as circumstances require. The findings and proposed ways forward below reflect the assessment done to date.

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

In the search for a reasonable solution for the right mix of the Total Force in the CMF, the Department assesses that the Services' proposed plans of approximately 37 RC teams, and hundreds of individual augmentees, would adequately support DoD cyberspace needs through FY 2018. USCYBERCOM has maintained that the most effective way to build the CMF is a build-assess-build model. As these RC teams are fully manned, trained, and equipped, continued assessment should occur to evaluate the developing role of RC personnel.

RC augmentation of the CMF will provide a more flexible workforce, by allowing for load sharing with active-duty forces and surge capacity with mobilization. The ability to plug in individuals from the RC as augmentees where needed, or to employ an RC-sourced team as a full CPT, allows DoD to leverage highly skilled industry personnel in the Reserve and Guard for the CMF. Continuing to build the RC forces inherently creates a surge capacity for the Department. It is possible these teams would look to support other cyberspace areas not solely focused on the CMF. These areas might not require "full time" engagement, but they may have the potential for aiding in maintaining situational awareness. Under this construct, the CMF would always be manned and trained to full capacity, and will continue to employ the world's most elite cyberspace operators.

- *Way Forward:* To take full advantage of the surge capacity created under this construct and to build additional Service capability, DoD should ensure that all cyberspace personnel, both Active and Reserve Component, are trained to the same joint standard. This will require a more flexible training pipeline. The Cyber Training Advisory Council (CyTAC), co-led by OUSD(P&R) and USCYBERCOM, must evaluate current training programs available in the Military Departments, the laboratories, our interagency partners (including DHS and DOJ), and private industry to offer equivalency training events for RC personnel that would meet the same standard as those offered through the current

USCYBERCOM pipeline. Where possible, such training should be planned to be cost effective and support remote access to reduce travel expenses.

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

Currently, the National Guard contributes to their respective CNDSP cyber missions that are not directly tied to the three CMF missions. These activities, however, are critical enablers for the CMF to conduct its missions. There are other activities that are critical CMF enablers as well.

The ability of the National Guard to fuse national capabilities with local partnerships is necessary for a whole-of-Government and whole-of-Nation cybersecurity approach. A leading example of this is the partnership between the Kansas Adjutant General and the State Attorney General at the Kansas Intelligence Fusion Center (KIFC), a State organization that partners with a wide variety of local law enforcement, emergency response, and critical infrastructure stakeholders. Joint Force Headquarters-Kansas, staffed by Air and Army National Guard units, provides national-level assets and analysis in a Kansas State-funded SCIF at the Fusion Center. This arrangement has paid significant dividends, as appropriately cleared critical infrastructure personnel are able to leverage national intelligence community expertise and data to identify threats to their networks in a manner that does not impact privacy or civil liberties. The KIFC has provided substantial cybersecurity benefits for Kansas critical infrastructure while also generating local intelligence with national significance. As a result, KIFC intelligence reporting has received more requests for information from the Intelligence Community than any other fusion center – largely driven by its cyber reporting.

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

As discussed, previously, the NG will support the CMF and USCYBERCOM's three missions. Additionally, however, the National Guard is well-positioned to offer its expertise and support to the States in traditional missions like natural disasters as well as less traditional missions in cyberspace. The National Guard is an important institution within the DoD's cyber enterprise, and National Guard personnel can support three important cyber missions. Similar to U.S. Code provisions that permit DoD forces to support domestic missions related to supporting law enforcement, homeland defense, and DSCA-related cyber activities, National Guard personnel also could be used to perform these cyber missions in Title 10 or Title 32 status. State National Guard personnel could be used in State active duty status to perform related State cyber missions in support of civil authorities (including law enforcement authorities) if authorized by State and Federal law. Governors also have the ability to employ National Guard personnel independently in State active duty status to perform C/TAA functions in compliance with Federal and State law. While under State command and control (i.e., State active-duty or Title 32 status), National Guard personnel operate at the direction, and under the command, of the Governor concerned, but use of National Guard personnel in a Title 32 status to perform these activities requires Secretary of Defense approval.

In addition to legal considerations, there are policy implications to consider. When assessing the appropriateness of using NG for State cyber activities, DoD considers four policy criteria: 1) is it

necessary and appropriate, particularly if it requires DoD resources; 2) is the infrastructure or asset critical to national security; 3) is the threat real and credible; and, 4) is there an adverse impact on readiness if NG personnel are supporting other activities.

If permitted by State and Federal law, when the Secretary of Defense determines that it is appropriate to employ National Guard personnel in Title 32 status, the Secretary of Defense may authorize, with the concurrence of the Governors of the affected States, National Guard personnel may be used to provide support to law enforcement, homeland defense, and DSCA activities. NG personnel (NG military in full-time and part-time status, military technician, or non-dual status technicians) could emphasize a coordinate, train, advise, and assist (C/TAA) role with State or local agencies, or private industry entities, depending on what is authorized by the Governor and the Secretary of Defense. While in this status, coordination and communication with Federal authorities are critical to enabling a whole of Government response. These C/TAA functions may include, but are not limited to, assisting such entities in cybersecurity planning, and providing subject-matter expertise in network defense and network security, cyber forensics, and response to cyber incidents without directly operating on private-sector networks. In so doing, the National Guard contributes to the defense and security of domestic critical infrastructure.

*Law Enforcement Support for cyber:* When operating in Title 32 status, National Guard personnel would not violate Section 1385 of Title 18, U.S. Code (the "Posse Comitatus Act"). The Posse Comitatus Act prohibits direct civilian law enforcement support by Army and Air Force personnel unless otherwise authorized by law (DoD policy has extended this prohibition to Navy and Marine Corps personnel). The law permits DoD personnel to provide certain kinds of civilian law enforcement support, including providing information collected during military operations or training to civilian law enforcement personnel; training and advising civilian law enforcement personnel; maintenance and operation of equipment for civilian law enforcement personnel; and support to the Attorney General related to weapons of mass destruction. NG personnel also may support DOJ, DHS, other Federal agencies, State agencies, or local agencies with law enforcement responsibilities at the request of the Governor, if appropriate and permitted by State and Federal Law. As demonstrated at the CYBER GUARD 14-1 exercise, sponsored by USCYBERCOM, there may be a role for NG personnel to play in supporting these law enforcement activities, including providing support to Federal, State, and local law enforcement agencies leading an investigation.

Under limited circumstances, it would be appropriate for DoD to work with civilian law enforcement agencies after cyber incidents, specifically in cases of terrorism or nation state attacks on national critical infrastructure, in DoD's role leading the military defense of the United States. Such attacks would directly affect national security, and may ultimately require DoD response, or, at least, awareness.

*Homeland Defense for cyber:* DoD relies on the Total Force to provide for the defense domains of the homeland. The National Guard is a vital element of the Total Force, and can be called upon to execute homeland defense missions in a Title 10 or 32, Section 902 duty status. Although this provision of law has not yet been used, it is possible that the Secretary may

determine that Total Force sourcing protection of national critical infrastructure or other assets is most appropriately conducted by National Guard units under State command and control. National Guard personnel also could perform homeland defense missions in a title 10 status supporting a Combatant Commander.

*Civil Support and Defense Support of Civil Authorities (DSCA) for cyber:* The Department of Defense defines DSCA as defense support to lead Federal agencies, consistent with the National Response Framework and the Presidential Preparedness Goal. Defense support comes from Total Force sourcing and could be executed by National Guard units or personnel operating in a Title 10 or 32 duty status.

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

As discussed in the "Current Status" section of this report, DoD has clearly defined Command and Control (C2) for the CMF and AC cyber units. However, work is required to determine what the best communication and coordination is for cyber teams when not operating in Title 10 status. Additionally, CYBER GUARD 14-1 demonstrated that there are communication and coordination challenges among DoD, other Federal, and State departments and agencies, and with the private sector when supporting whole-of-Government and whole-of-Nation cyber responses and activities.

Well-established coordination and communication with interagency partners, and clear lines of authority to the appropriate Combatant Commander, are critical for the RC to be able to contribute to the national mission. Although the exact placement of each RC team operating in a Title 10 status in the C2 structure depends on the mission assigned to the individual team, RC teams operating in State active duty or Title 32 status do not fall within the DoD C2 structure at all, and there is no unity of command because the Guard units would fall under State control.

The Joint Staff, working with USCYBERCOM, USNORTHCOM, USPACOM, USSTRATCOM, the Services, and the National Guard Bureau, will propose the appropriate coordination and communication lines of efforts for NG teams operating under State control and report to the Department when required during the planned reassessment of the direct support model in FY 2015.

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

Since cyber is a highly technical domain, recruiting and retaining the most highly skilled technical personnel continue to be top priorities for the Department. Although the Military Departments/Services established plans to recruit highly skilled military personnel, a new corps of civilian employees with technical cyber skills is vital to the establishment of an elite cyberspace workforce capable of responding to threats in cyberspace.

DoD needs to hire full-time highly-technical civilian employees as engineers, systems/technology developers, researchers, and systems/technology implementers. Therefore,

we assess, in the near term, that DoD needs to develop a long-term solution to recruit, retain, and grow a highly skilled technical civilian workforce and have flexible human resources management authorities to govern these individuals. Since military personnel serve in military billets on a temporary basis, these full-time civilians employees would become the backbone of continuity for the DoD cyber technical workforce. This would directly contribute to CMF readiness and support DoD's ability to prepare for, plan, and execute its missions.

DoD requires a long-term solution to ensuring that its force comprises the best and brightest technical experts. Special hiring authorities may be necessary to entice such individuals from outside of government to support USCYBERCOM and the Military Departments/Services as subject-matter experts to support engineering, development, implementation, integration, and conduct of cyberspace operations.

- *Way Forward:* DoD would benefit from special hiring authorities for DoD civilians. The Air Force, as the executive agent of USCYBERCOM, and the other Military Departments/Services all contribute technical personnel to the CMF and therefore may benefit from special hiring authorities. Considerations for such authorities include:
    - *Special Pay:* DoD would review civilian cyber skillsets to identify and prioritize the occupational specialties to be targeted for special pay. One key group of civilian employees on which to focus are those with responsibilities to integrate technological solutions across the entire DoD enterprise. For these and others in the most critical occupational specialties who qualify for these jobs, salaries and incentives should be commensurate with their colleagues in the private sector, including bonuses, tuition payback, and relocation expenses. Additionally, Congress should consider a special cyber salary rate table to affect compensation across a wider subset of civilian employees in cyber-related fields. Implementation of any special incentives should include an objective way to realign the existing civilian workforce into high-priority workroles to ensure that the best qualified employees are retained. Special pay should be based on the mission required, not necessarily by an individuals' occupational series.
    - *Flexible assignment policies:* DoD would explore establishing regular opportunities for civilian employees to move between organizations with cyber-enabling national security employment opportunities. Home organizations should have the authority and be incentivized to permit rotation of their civilian employees with other parts of the national cyber enterprise, including the IC, DHS, and DOJ. These rotations would provide DoD technical subject matter experts with a variety of professional development and interagency experience. Once implemented, these policies also could be useful retention tools to keep highly-motivated civilians within the U.S. Government.
    - *Security clearances:* Security clearances remain an essential aspect of vetting government employees to fill critical national security positions. Although there is no substitute for a thorough review of a potential employee's background, those applicants applying for jobs in critical specialties should have their reviews

prioritized. Lengthy background checks create uncertainty for Federal applicants and can deter those with competing employment offers from completing a Federal application – a process which can take more than 12 months.

*Finding: Training and equipping the cyber Total Force may require additional capability*

USCYBERCOM's has relied historically on the IC for training and on platforms used to conduct operations for the IC, but the Department has chosen to invest in an independent training pipeline and diverse platforms to conduct USCYBERCOM's three missions. These investments will ensure that the CMF has the infrastructure it needs to carry out its missions and will result in a variety of diverse, highly scalable, easily deployable, and disposable platforms capable of information sharing across cyberspace military operations.

*Training:* DoD cyber forces require an accessible, persistent cyber training environment with sufficient capacity to ensure that geographically dispersed teams are fully prepared for future scenarios involving cyberspace operations. Teams, including civilian and RC personnel, must routinely practice assigned or anticipated missions on designated training networks that simulate or replicate select contingency scenarios. A persistent cyber training environment requires designated space and equipment, with access to operationally realistic cyber capabilities and training networks. Such an environment would be conceptually similar, only in a virtual sense, to a "range" on which traditional military units train and exercise military tasks in a controlled environment, and assess performance. The persistent training environment should be remotely accessible, quickly programmable/reprogrammable, capable of simulating an adversary's, or other, computer network environment, and should emulate cyber attacks on DoD networks, critical infrastructure, or other computer systems. This persistent cyber training environment would teach specific skills and use of systems as part of individual and team qualification to execute core cyber competencies through execution, examination, and evaluation similar to how an aviator develops skills in a flight simulator or an Army infantry unit trains at the Joint Readiness Training Center.

The requirement for a persistent cyber training environment is not limited to active-duty forces. On the contrary, although many RC personnel possess sophisticated technical expertise in computer networks, they require routine access to specialized training required to perform their military duties. For example, many Reserve and National Guard participants at the 2014 CYBER GUARD exercise stated that it had been several months since they had employed the tools used in the exercise. To address this challenge, RC cyber units require remote and/or virtual access to the same persistent cyber training environment used by AC forces. RC units could use existing facilities and network infrastructure on or near their home station to access remotely and virtually the training environment and underlying cyber training ranges that emulate cyber attacks on simulated networks.

- *Way Forward:* DoD will examine and articulate the requirements for a persistent training environment while leveraging existing ranges and resources to the maximum extent practicable. If additional resources are needed, the Department will examine them in its program and budget review process.

*End-to-end, integrated architecture plan:* DoD currently has multiple ongoing requirements definition efforts, material solutions analysis, and programs to support the equipping of cyber forces, including joint cyber situational awareness, interagency data and information sharing, C2 for cyberspace operations, and platforms to conduct operations. Although DoD is investing in all of these components, a joint solution is necessary.

- *Way forward:* DoD will develop a capability roadmap and implement an architecture plan leveraging expertise from the private sector, both from technical subject matter experts and implementers, and to the maximum extent possible existing commercial technical solutions.

## Cost Assessment

Although there is an upfront accepted cost to the Army and Air Force to implement their plans to provide CMF surge capacity, to hire and train personnel for unique non-CMF missions, and, when authorized, to provide support to protecting national critical infrastructure, these investments may yield savings in the long term. Each of these mission areas must be continuously examined on a case-by-case basis to maintain the appropriate force mix as cyberspace operations mature. As discussed earlier in this report, cost is only one factor to consider when determining the appropriate force structure and force mix.

One example of how the Department should consider all factors on a case-by-case basis is by examining the potential difference in duty rotation among the Active and Reserve Components. In some cases, the average AC rotation schedule is approximately three years, while the average RC recurring training costs are extrapolated over approximately nine years. Accordingly, and conceptually similar to DoD civilians, some RC personnel with cyber expertise from their civilian professions may be able to perform in the same work roles in their DoD capacity for nearly three times as long as their AC counterparts. In this example, taking advantage of longevity may decrease the cost of training over the years and increases the level of proven expertise and continuity of knowledge across the Total Force.

Other situations might call for different factors to be considered. Although RC personnel could be helpful to the Department during cyber crises, they might be more helpful to the Nation by remaining at their civilian jobs if the companies they work for are part of the crisis. For example, if Microsoft has been attacked, a Guardsman or Reservist who works for Microsoft might be better suited to help Microsoft fix the situation as part of his or her civilian professional capacity rather than leaving Microsoft to perform a related DoD mission, such as supporting DHS efforts in assisting Microsoft.

Examples like the ones above illustrate the complexity of the factors that will need to be considered by the Department in the future.

## Conclusion

The readiness of the CMF remains DoD's top cyber priority. The Department recognizes the need to incorporate the strengths, skills, and authorities afforded to the Reserve Components into

the overall cyber force structure. USCYBERCOM and the Military Departments/Services have made significant progress over the past 18 months. However, they must continue to develop an integrated military and civilian Total Force response to achieve USCYBERCOM's three missions, and, when necessary, to support DoD's Federal partners, as informed by State cyber mission needs. Although initial analysis has been conducted, additional assessment will occur in FY 2016 and beyond once the CMF is well on its way to being fully manned, trained, and equipped.

# Annex 1: Air Force Reserve Component Units

## 960th Cyber Operations Group Units

These locations were selected based on the existence of infrastructure for these part-time positions and the availability of SCIF space.

- *960th Cyber Operations Group (Texas).* Mission: C2 of subordinate squadrons. 42 authorized personnel;
- *860th Network Operations Squadron (NOS) (Virginia)* and *960th Network Operations Squadron (Colorado).* Mission: Defend Air Force networks and uphold Air Force and DoD standards to ensure network availability. 62 authorized personnel (860th NOS); 72 authorized personnel (960th NOS).
- *854th Cyberspace Operations Squadron (Texas).* Mission: Full-spectrum cyber operations and capabilities in support of Air Force and Joint requirements. 101 authorized personnel;
- *426th Network Warfare Squadron (Texas*). Mission: To produce effects for the Air Force and CCMDs in, through and from cyberspace by employing synchronized network defense operations to detect, respond, and prevent network intrusions. 157 authorized personnel;
- *960th Network Warfare Flight (NWF) (Nebraska)* and *860th Network Warfare Flight (Texas).* Mission: Provide personnel to monitor Air Force communications computer systems for adversary value. 35 authorized personnel (960th NWF); 39 authorized personnel (860th NWF)

## Air National Guard Units

- *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; and
- *177th Information Aggressor Squadron (Kansas).* Mission: Red teaming assessments.

# Annex 2: Reserve Component Infrastructure

## Army Reserve Components

The USAR is using existing infrastructure to support cyber missions such as: the ARIOC consisting of 308 personnel, headquartered in Adelphi, Maryland with five battalions distributed nationwide; the USCYBERCOM-U.S. Army Reserve Element (ARE), which has capacity for 23 personnel located at Fort Meade, Maryland; and the DISA ARE with 111 total personnel (57 personnel at Ft Meade, 18 personnel at Redstone Arsenal, Alabama, 18 personnel at Fort Carson, Colorado, and 18 personnel at Scott AFB, Missouri). As discussed earlier, the ARNG is leveraging the following infrastructure to perform cyber missions: the Virginia DPU with its 174 personnel in Manassas, Virginia, the ARNG Title 10 team in Laurel, Maryland with capacity and connectivity for 43 personnel. This is in addition to forces possessed by each State and territory such as JFHQ-DOIMs consisting of 1,160 total personnel and State Cyber Network Defense-Teams with a total strength of 432 personnel. The USAR and ARNG are also assessing their additional infrastructure assets for future use by the RC's CMF. The USAR plans to locate their CPTs within the facilities currently used by the ARIOC. The ARIOC has subordinate infrastructure located in: Adelphi, Maryland; Pittsburgh, Pennsylvania; Devens, Massachusetts; Fort Sam Houston, Texas; and Camp Parks, California. Each of these facilities can accommodate and provide connectivity for 59 personnel. This presents a potential requirement to increase capacity or connectivity at each location to account for future CPT capacity.

## Air Force Reserves

Air Force Reserve cyber personnel work in the same infrastructure space as their active-duty counterparts greatly reducing, and in many cases eliminating, infrastructure needs.

## Navy Reserves

Reserve units work in the CMF leveraging access to command assets whenever possible. For those personnel and units not collocated with a gaining command, the Navy relies on the JRICs to provide the necessary infrastructure.

## Marine Corps Reserves

The Marine Corps Reserve personnel augment existing forces utilizing existing infrastructure within those commands.

## Annex 3: Acronym list

AAS – Associate in Applied Science
AC – Active Component
AFCYBER – Air Force Cyber Command
ARCOG – U.S. Army Reserves Army Cyber Operations Group
ARCYBER – Army Cyber Command
ARIOC – Army Reserve Information Operations Command
ARE – Army Reserve Element
ARNG – Army National Guard
ANG – Air National Guard
ASI – Additional Skill Identifier
ASVAB – Armed Services Vocational Aptitude Battery
C2 – Command and Control
C10F – Commander 10th Fleet
CCMD – Combatant Command
CFCOE – Cyberspace Forces Concept of Operations and Employment
CIMB – Cyber Investment Management Board
CJCS – Chairman of the Joint Chiefs of Staff
CMF – Cyber Mission Force
CMT – Combat Mission Team
CNDSP – Computer Network Defense-Service Provider
CND-T – Computer Network Defense Teams
CNO – Chief of Naval Operations
CoE – Center of Excellence
CoG – Council of Governors
COMINT – Communications Intelligence
C/TAA – Coordinate, Train, Advise, and Assist
CPT – Cyber Protection Team
CS/IA – Cyber Security / Information Assurance
CST – Combat Support Team
CTN – Cryptologic Technician Networks
CVA – Cyber Vulnerability Assessment
CWE – Cyber Warfare Engineer
CyOG – Cyber Operations Group
CyTAC – Cyber Training Advisory Council
DCO – Defensive Cyber Operations
DHS – Department of Homeland Security
DIB – Defense Industrial Base
DISA – Defense Information Systems Agency
DoD – Department of Defense
DoDIN – Department of Defense Information Networks
DoJ – Department of Justice
DSCA – Defense Support of Civil Authorities
DSOC – 2011 Department of Defense Strategy for Operating in Cyberspace

ECS – Enhanced Cybersecurity Services
FCC/C10F – Fleet Cyber Command/Commander 10th Fleet
HRC – Human Resources Command
HQ – Headquarters
IASP – Information Assurance Scholarship Program
IC – Intelligence Community
IMA – Individual Mobilization Augmentees
IAS – Information Aggressor Squadron
IDC – Information Dominance Corps
IOS – Information Operations Support
IOSC – Information Operations Support Command
ISR – Intelligence, Surveillance, and Reconnaissance
IT – Information Systems Technician
ITEB – Individual Training Equivalency Board
ITP – Individual Training Pipeline
JCAC – Joint Cyber Analysis Course
JCRE – Joint Cyber Reserve Element
JCT&TS – Joint Cyberspace Training and Certification Standard
JFHQ-C – Joint Force Headquarters-Cyber
JFHQ-DOIM – Joint Force Headquarters-Directorates of Information Management
JIE – Joint Information Environment
JRIC – Joint Reserve Intelligence Centers
KIFC – Kansas Intelligence Fusion Center
KSA – Knowledge, Skills, and Ability
MOS – Military Occupational Specialty
NDAA – National Defense Authorization Act
NG – National Guard
NGB – National Guard Bureau
NICE – National Initiative for Cybersecurity Education Workforce
NMT – National Mission Team
NOS – Network Operations Squadron
NPS – Naval Postgraduate School
NRO – National Reconnaissance Office
NSA – National Security Agency
NST – National Support Team
NVCC ASI – Northern Virginia Community College Advanced Standing Initiative
NWF – Network Warfare Flight
NWS – Network Warfare Squadrons
OPM/NSF – Office of Personnel Management/National Science Foundation
OPNAVO – Office of the Chief of Naval Operations
OSD – Office of the Secretary of Defense
PCA – Principal Cyber Advisor
POM – Program Objective Memorandum
RC – Reserve Component
ROTC – Reserve Officer Training Corps

SCIF – Sensitive Compartmented Information Facilities
SEB – Selective Reenlistment Bonuses
SME – Subject Matter Expert
SPP – State Partnership Program
STEM – Science, Technology, Engineering, and Mathematics
T&R – Training and Readiness
TRADOC – Training and Doctrine Command
UCP – Unified Command Plan
USAFR – United States Air Force Reserve
USAR – US Army Reserve
USCYBERCOM – United States Cyber Command
USSTRATCOM – United States Strategic Command
USMA – United States Military Academy
UTC – Unit Type Code
VA DPU – Virginia Data Processing Unit

## Annex 4: 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.