Department of Defense

Cyberspace Workforce Strategy

December 4, 2013

Forward

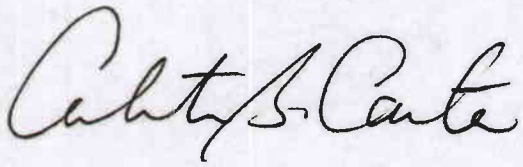
As adversaries exploit the Cyberspace domain for their military, economic, and political advantage, operations in cyberspace are evolving from an afterthought to a fundamental element for achieving all missions. The Department must similarly evolve the workforce to address the needs of the domain.

The Department of Defense (DoD) Cyberspace Workforce Strategy (DCWS) is the overarching enterprise guidance for transforming the cyberspace workforce of military (active/reserve) and civilian personnel and includes approaches to recruit, train and retain staff in a competitive national environment. The DCWS focuses efforts in order to establish workforce requirements, produce consistency and applicability of cyberspace skills and abilities, as well as promote a greater understanding of cybersecurity responsibilities as technology advances.

To transform the cyberspace workforce the DCWS focuses on six key areas:

- ***Establish a cohesive set of DoD-wide cyberspace workforce management issuances.*** Establishing a single set of DoD policies and directives for building a qualified and adaptable cyberspace workforce
- ***Employ a multi-dimensional approach to recruiting.*** Adopting innovative recruitment methods such as assessing aptitude and creating DoD transition opportunities
- ***Institutionalize continuous learning with greater focus on evaluating the maturity of skills.*** Combining diverse learning methods to maintain a qualified cyberspace workforce keeping pace with the evolution of activities and technologies within the domain
- ***Retain qualified personnel.*** Developing and retaining cyberspace professionals by offering a wide range of career and training opportunities and compensation packages to transform DoD into an employer of choice
- ***Expand threat knowledge.*** Ensuring the cyberspace workforce has the understanding of current threats and situational awareness needed to make responsible decisions when working in cyberspace
- ***Understand crisis and surge requirements and options.*** Conducting mission analyses and considering how to best leverage the cyber skills of the Reserve, National Guard, DoD Civilians, as well as examining options for leveraging personnel within the Defense Industrial Base (DIB) and other parts of the private sector

Executing the DCWS will require a commitment to continued and increased cooperation and collaboration across the Department and the cyberspace community. Collectively we can achieve success as we cultivate the workforce to address current and future demands.



DoD Cyberspace Workforce Strategy

Introduction

Cyberspace is acknowledged as a warfighting domain of mission critical importance to the DoD. As adversaries exploit this domain for their military, economic, and political advantage, operations in cyberspace are evolving from an afterthought to a fundamental element. The cyberspace workforce[1] is similarly evolving, from supporting work roles to positions that are recognized as critical to the defense of the nation and it is comprised of personnel who build, secure, operate, defend, and protect DoD and U.S. cyberspace resources; conduct related intelligence activities, enable future operations and project power in or through cyberspace. This includes a subset of the intelligence workforce and portions of the DoD workforce with legacy names such as Network Operations workforce, Information Technology workforce, Information Assurance (IA) workforce, Engineering workforce, etc. This evolution is reshaping the requirements for all personnel working in cyberspace; for example, by integrating responsibilities to protect cyberspace into every work role.

This document is the Department's strategy for transforming its cyberspace workforce of military (active/reserve) and civilian personnel and includes approaches to recruit, train and retain staff in a competitive national environment. Additionally, many of the principles and tenets within this document will hold true for the contract services supporting the Department's cyberspace workforce personnel. Successful execution of this cyberspace workforce strategy requires coordinated action across the Department, the Office of Personnel Management (OPM), agencies, industry partners, and academia, while keeping Congress informed. This document amplifies the workforce aspect of *DoD Strategy for Operating in Cyberspace* (July 2011) and supplements *Defense of DoD Networks, Systems, and Data: Strategic Choices for 2020*.

> "The development and retention of an exceptional cyber workforce is central to DoD's strategic success in cyberspace."
>
> – DoD Strategy for Operating in Cyberspace, July 2011

[1] Cyberspace Workforce definition will be reviewed, updated and published in future DoD issuances, as the cyberspace domain, missions, and workforce evolves.

Situation

There is a recognized pervasive national shortage[2] of skilled cyberspace personnel, potentially impacting the operational readiness across the Department and putting national security at risk. Despite the vast expansion of cyberspace educational and experiential opportunities available, the Nation's cyberspace talent pipeline remains limited. Due to this shortage, DoD is collaborating with other government agencies, industry and academia to address the "cyberspace talent pipeline" challenge. While working collaboratively with these entities, DoD faces fierce competition within the labor market to secure the highly-skilled experts needed from the Nation's finite talent sources. In light of this competition, DoD must endeavor to brand itself an "employer of choice." To do so, the Department must seek to foster an environment where revolutionary innovation, enabled through cutting-edge technologies, produce a world-class workforce ready to meet any and all cyberspace challenges.

Concurrently, DoD must expand educational and training opportunities to cultivate talent from within the Department. Continuous organizational and individual learning needs to be the norm, reinforced by relevant content that enables proficiency training, on-the-job training, exercises, and expanded use of cyberspace ranges, all of which place emphasis on obtaining and maintaining qualifications. A successful career needs to be obtainable via multiple paths. Career progression needs to be flexible, with a rich diversity of job and career opportunities including leadership, non-technical, and technical.

Global mission challenges call for standardized work roles and common training requirements. Yet in this new cyberspace domain, most work roles remain DoD Component-specific. As challenging as it has been to manage current divergent cyberspace workforce requirements, the Department recognizes the demand to reevaluate staffing requirements, realign personnel within cyberspace work roles, and retain skilled and qualified personnel. Many current civilian occupational series and military occupational specialty codes are broadly defined, spanning a wide variety of skills and aligned with legacy work roles, functions, and positions. Without specific characterization of work roles and qualifications, it is difficult to identify resource requirements, assess personnel readiness, and maintain cyberspace skills. These work roles and qualifications must apply to civilians, military personnel, as well as those functions augmented or being met through contract support.

To aid in this effort, the U.S. Cyber Command (USCYBERCOM) has identified cyberspace work roles and developed workforce qualification requirements specific to their mission needs. These efforts will be integrated into the overarching DoD Cyberspace Workforce Framework and will be part of a persistent mission analysis to improve the understanding of the type and volume of skills needed to execute missions.

Despite current workforce challenges, today the DoD has some of the best, most advanced cyberspace personnel and capabilities in the world. Advanced DoD missions and capabilities offer unique opportunities, and must be marketed accordingly to potential candidates and existing personnel. This strategy provides the foundation to address DoD needs by leveraging departmental strengths.

[2] Center for Strategic and International Studies, *A Human Capital Crisis in Cybersecurity— Technical Proficiency Matters* (Washington, D.C.: April 2010).

Strategic Focus Areas

This DoD Cyberspace Workforce Strategy contains six strategic focus areas for building and maintaining a competent and resilient cyberspace workforce. Success in cyberspace is dependent on having a knowledgeable and skilled workforce that can adapt to the dynamic environment and adjust resources to meet mission requirements. The first five focus areas address steady-state operations, and the last focus area addresses workforce needs for crisis and surge support:

1. **Establish a cohesive set of DoD-wide cyberspace workforce management issuances.** A single set of DoD policies and directives will be established, reconciled with existing IT/IA, Intelligence and Operations policies and directives, for building a qualified and adaptable cyberspace workforce. This is a key strategic point required to set the cyberspace workforce standards and guide the Department; by identifying cyberspace work roles, the required qualifications, and parameters for managing the workforce.
2. **Employ a multi-dimensional approach to recruiting.** The Department will adopt innovative recruitment methods such as assessing aptitude and creating DoD transition opportunities. DoD will also partner with DHS and the federal sector to develop the national cyberspace talent pipeline.
3. **Institutionalize continuous learning with greater focus on evaluating the maturity of skills.** The Department will combine diverse learning methods (skill-based, on-the-job, exercise-based, etc.) to maintain a qualified cyberspace workforce keeping pace with the evolution of activities and technologies within the domain.
4. **Retain qualified personnel.** The Department will develop and retain cyberspace professionals by offering a wide range of career and training opportunities and compensation packages to transform DoD into an employer of first choice. Retention is a key area that the Department will monitor with the goal of constant and steady improvement.
5. **Expand threat knowledge.** The Department must ensure the cyberspace workforce has the understanding of current threats and situational awareness needed to make responsible decisions when working in cyberspace.
6. **Understand crisis and surge requirements and options.** As part of conducting a mission analysis, the Department will consider how it could best leverage the cyber skills of the Reserve, National Guard, DoD Civilians, and examine options for leveraging personnel within the Defense Industrial Base (DIB) and other parts of the private sector.

Table 1: Summary list of strategic focus areas for building a competent and resilient cyberspace workforce

Focus Area 1: Establish cohesive set of DoD-wide cyberspace workforce management issuances		
From: DoD-wide Information Assurance (IA) personnel workforce policies	To: DoD-wide cyberspace workforce policies that establish common work roles and qualifications for all cyberspace positions	Critical Elements: • Create the DoD Cyberspace Workforce Framework (CWF) as the standard lexicon for cyberspace work roles. • Establish overarching cyberspace workforce management issuances. • Establish workforce management requirements for identifying and tracking personnel and qualifications within the cyberspace workforce. • Establish position description criteria for cyberspace positions and personnel; and include in appropriate guidance.

Focus Area 2: Employ a multi-dimensional approach to recruiting		
From: Traditional cyberspace recruiting based on general personnel qualifications	To: Targeted and non-traditional recruiting based more on aptitude and specialized skills	Critical Elements: • Partner with DHS and the federal sector to develop a national cyberspace talent pipeline. • Assess aptitude as well as qualifications. • Create transition opportunities between and within military and civilian service. • Develop awareness of the unique cyberspace workforce opportunities at DoD. • Foster non-traditional hiring for niche mission needs.
Focus Area 3: Institutionalize continuous learning with greater focus on evaluating the maturity of skills		
From: Static training and certification/qualification without practical application requirements	To: Dynamic, relevant, continuous learning to maintain currency, with training and certification closely aligned with mission needs	Critical Elements: • Manage cyberspace training standards and requirements. • Institute proficiency development and measurement. • Identify and leverage Department-wide training and education opportunities. • Expand cyberspace learning requirements to all Department leaders. • Establish an environment fostering continuous learning and professional development. • Provide for individual and collective training in a realistic and persistent simulated environment. • Incentivize development of specialized training.
Focus Area 4: Retain qualified personnel		
From: Ongoing determination of cyberspace structure and retention needs.	To: A wide range of cyberspace career opportunities and meaningful challenges	Critical Elements: • Provide career progression and meaningful challenges. • Offer training opportunities tied to retention commitments. • Retain qualified performers via compensation programs. • Identify and retain cyberspace leaders.
Focus Area 5: Expand threat knowledge		
From: IA focused annual training	To: Increased cyberspace threat knowledge focused on current threat data, individual responsibilities	Critical Element: • Institute a cyber-threat knowledge program across DoD. • Establish standards and methods for individual reporting of potential cyberspace issues. • Test and evaluate cyber-threat awareness.
Focus Area 6: Understand crisis and surge requirements and options		
From: Unknown surge capacity and requirements	To: Understanding of crisis and surge support requirements, and options for leveraging external partner expertise and capacity.	Critical Elements: • Analyze Reserve and National Guard support for cyberspace missions. • Explore options to leverage DoD Civilians cyber expertise. • Identify options for accessing DIB sector cyber expertise. • Investigate options for accessing cyber expertise from other Public-Private partners.

Focus Area 1: Establish a cohesive set of DoD-wide cyberspace workforce management issuances

While the military Services and DoD Components have management processes and guidance that address all personnel (military and civilian), including personnel assigned to positions within the cyberspace workforce, there is no OSD guidance that specifically addresses the scope of the cyberspace workforce. Guidance exists for areas such as information assurance, but that is a subset of the yet to be fully defined cyberspace workforce. The building blocks of a capable, prepared and adaptive cyberspace workforce are the policies and directives that outline work roles and qualifications. This is a strategic point of leverage, in that standardized work roles and qualifications enable the unity and interoperability needed for consistent understanding, common training and joint operations.

New policies and directives will be developed and reconciled with existing IT/IA, Intelligence and Operations policies and directives, to address workforce management requirements for technical, non-technical, and leadership work roles across all areas of the cyberspace workforce and will apply to active and reserve component military, DoD civilian employees, as well as certain elements of contract support (as appropriate and consistent with delineated contractual requirements). While these policies and directives will provide the scope, description of work roles, baseline qualifications, and workforce management requirements for the cyberspace workforce; each DoD Component will still be responsible for determining how to best organize and employ their cyberspace workforce to address their mission requirements. These new policies and directives will draw upon and support broader initiatives such as those driven by the Comprehensive National Cybersecurity Initiatives (CNCI) and the DoD Strategy for Operating in Cyberspace (DSOC).

Critical elements for developing a cohesive set of Department-wide cyberspace workforce management policies and directives are: (these critical elements will drive the requirements for Focus Area 3)

- **Create the DoD Cyberspace Workforce Framework (CWF) as the lexicon for cyberspace work roles.** The DoD needs consistency when defining cyberspace work roles and qualifications to enable staffing for effective mission execution, particularly in joint environments. Therefore, the DoD CIO will lead a working group of representatives from Department components to develop the DoD CWF. The DoD CWF will be based on the integration of the National Initiative for Cybersecurity Education (NICE) workforce framework[3] and the Joint Cyberspace Training and Certification Standards (JCT&CS),[4] both of which reflect foundational contributions from the National Security Agency, to provide a lexicon of work roles by area of specialty, each with a baseline set of required knowledge, skills, and abilities (KSA) as well as functions. DoD CWF specialty codes will be developed for each cyberspace work role. The DoD CWF will be implemented across the Department to facilitate the identification of personnel in cyberspace work roles. The DoD CWF will be a "living document," reviewed annually and updated as necessary to reflect evolving DoD mission and workforce requirements. Additionally, an implementation plan will be developed to address transition to the standardized work roles; as well as the relationship of work roles to positions and missions.

[3] The National Initiative for Cybersecurity Education (NICE) developed the National Cybersecurity Workforce Framework to provide a common understanding of and lexicon for cybersecurity work.

[4] The Joint Cyberspace Training and Certification Standards (JCT&CS) signed in February 2012 established complementary joint training and certification standards for the cyberspace workforce with inputs to policy revisions.

- **Establish overarching cyberspace workforce management issuances.** DoD Directive 8570.01 "Information Assurance Training, Certification, and Workforce Management" and its corresponding manual DoD 8570.01-M "Information Assurance Workforce Improvement Program" do not reflect all of the work roles and qualifications needed to achieve the cyberspace mission. These issuances are intended to address only IA work roles. The CWF stated above will identify the full spectrum of cyberspace workforce roles. Therefore, these issuances must be replaced, supplemented, or broadened as the Department develops policy for the entire cyberspace workforce. Additional issuances will be developed and reconciled with existing IT/IA, Intelligence and Operations policies and directives, as needed to provide specific qualification and credentialing requirements for the work roles. These foundational tools will support DoD's ability to collectively and strategically plan for the cyberspace workforce of the future.
- **Establish workforce management requirements for identifying and tracking manpower, personnel and qualifications within the cyberspace workforce.** Once cyberspace work roles are developed, the Department will establish manpower and personnel identification and tracking requirements. DoD components will be responsible for evaluating their cyberspace personnel; identifying, designating, and tracking those who are highly-skilled. These new workforce management requirements will be leveraged to understand staffing needs and assist with identifying future assignments. Additionally, DoD components will be responsible for determining the best course of action for implementing these new requirements in Department manpower, personnel, and readiness databases.
- **Establish position description criteria for cyberspace positions and personnel in appropriate guidance.** Every person in a cyberspace work role has cybersecurity responsibilities. Position description criterion will include roles identified in the DoD Cyberspace Workforce Framework and the cybersecurity responsibilities within each role. Contract service requirements will also be updated to include cybersecurity responsibilities for all cyberspace work roles (technical, non-technical and leadership), per CWF. For example, a system administrator would have a clear understanding of his or her responsibilities for hardening and maintaining the integrity of systems, software, and networks; as well as for identifying suspicious cyber activity (anomaly detection), analysis and escalation. Employee union/bargaining unit representatives, as well as private sector representatives, will be notified and involved as appropriate.

Focus Area 2: Employ a multi-dimensional approach to recruiting

> "*DoD will catalyze U.S. scientific, academic, and economic sources to build a pool of talented civilian and military personnel to operate in cyberspace and achieve DoD objectives.*"
>
> – *DoD Strategy for Operating in Cyber*space, July 2011

As the Department matures its cyberspace doctrine, recruiting programs must be recalibrated in order to continuously sustain workforce requirements. The DoD must approach identifying and recruiting candidates as a long term transformational effort. Development of the CWF and policies addressed in Focus Area 1 will allow the Department to better characterize the work roles and qualifications necessary for an effective workforce. However, the Department must build on that foundation to motivate students and professionals to pursue education and career opportunities in

the cyberspace domain and to view DoD as an employer of choice for the duration of their career. Expansion of current recruiting practices to identify aptitude and critical skills provides the opportunity to apply talent to the appropriate cyberspace work roles. Finally, the DoD will encourage career transitions into cyberspace work roles and establish incentive programs, as necessary, for cyberspace talent in critical work roles.

Critical elements for transforming DoD workforce recruitment approaches are:

- **Partner with DHS and the federal sector to develop a national cyberspace talent pipeline.** In March 2011, the Commander of U.S. Cyber Command, General Keith B. Alexander, testified that the military did not have enough highly skilled cyberspace personnel to address the current and future cyberspace threats to our infrastructure or to conduct full spectrum military cyberspace operations. General Alexander stated that one of the most critical cyberspace issues confronting U.S. Cyber Command is the need for collaborative force development so that, when directed, freedom of action can be denied in cyberspace to our adversaries.[5] In 2010, the Center for Strategic and International Studies reported a shortage of qualified cybersecurity professionals in the United States, including those who can design secure systems, write secure computer code, and create the tools needed to prevent, detect, mitigate, and reconstitute information systems.[6] While there have been improvements this shortage persists today and it is for these reasons, DoD will:
    - Partner with DHS and the federal sector, to establish outreach, mentoring and literacy programs to develop critical skills and significantly increase awareness of cyberspace opportunities
    - Endorse and sponsor games, competitions, fairs, conferences and camps to create educational growth paths
    - Directly link scholarships (e.g., IA Scholarship Program), internships and fellowships to federal opportunities
    - Leverage Reserve Officers' Training Corps (ROTC) programs and the Service Academies to inject more cyberspace elements, seek more cyber-related majors, and, where applicable, place them in cyberspace jobs once commissioned

  Investment in the workforce of the future benefits the nation at large and expands the talent pipeline of potential recruits.
- **Assess aptitude as well as qualifications.** Not all successful cyberspace personnel will have a Science, Technology, Engineering and Math (STEM) background. Rather, a broad range of experiences can lead to a qualified cyberspace employee. The Department must develop methods to assess aptitude (critical thinking and problem-solving ability) as a tool for recruitment in addition to using traditional knowledge-based qualifications for both military and civilian positions (Note: aptitude assessments may not be applicable for all cyberspace work roles). To ensure the success of future DoD cyberspace recruiting efforts, the DoD will:
    - Evaluate the availability and/or development of assessment tools that would replace or augment existing capabilities to identify military and civilian candidates for cyberspace work roles
        - Using the Defense Language Aptitude Battery as one of the models for aptitude assessments (evaluating the ability to learn a language vice having previous knowledge of a language)

[5]General Keith B. Alexander, in a statement before the House Committee on Armed Services, Subcommittee on Emerging Threats and Capabilities, Washington, D.C., March 16, 2011.

[6]Center for Strategic and International Studies, *A Human Capital Crisis in Cybersecurity— Technical Proficiency Matters* (Washington, D.C.: April 2010).

- Explore updating the knowledge-based Armed Service Vocational Aptitude Battery (ASVAB) exam to identify those military recruits who may have an aptitude for cyberspace work roles
    - Tapping into those with aptitude, rather than just those with appropriate qualifications, will expand the pipeline of available talent for entry-level positions and those seeking to switch career tracks

- **Create transition opportunities between and within military and civilian service.** While developing the next generation of the cyberspace workforce is critical to long-term success, the Department must also develop ways to realign and transition its current workforce by recruiting them into diverse cyberspace positions. To accomplish realignment and transition of the current cyberspace workforce, DoD will:
    - Develop methods to cross-train government personnel who have the interest and the aptitude for cyberspace positions
    - Ensure commonality in the application of workforce mix criteria and considerations across the domain in an effort to standardize the classification of work roles to facilitate the most appropriate, flexible, responsive, and cost effective allocation of functions among the Total Force of military (active or reserve), civilians, and contract support, consistent with the sourcing authorities and policies of the Department.
    - Actively engage cyberspace personnel leaving the military – by cooperating with the Transition Assistance Program (TAP) Office and leveraging authorities/initiatives such as Veteran's Opportunity to Work (VOW)/Veteran's employment Initiative (VEI) – during their transition period to ensure their awareness of Reserve, National Guard, and civil service opportunities to retain the critical skills and experience within the Department. Re-address the applicability of physical requirements for retention of wounded, ill, and injured service members in active duty cyberspace positions[7]
        - There is an untapped wealth of knowledge and aptitude among wounded, ill, and injured service members, as well as a desire for continued service. Current identification, recruitment, selection, and retention of military personnel places a premium on physical ability/attributes. Through the Integrated Disability Evaluation System (IDES) process some wounded, ill, or injured Service members could be found fit and retained to serve in uniformed cyberspace positions.
- **Develop awareness of the unique cyberspace workforce opportunities at DoD.** The DoD has a unique cyberspace mission that involves world-class offense, defense, network operations, and cyber-related intelligence activities, often in classified environments. The opportunity to work in these unique mission areas in the defense of our nation will attract candidates as they see the benefits, opportunities, and challenges offered by a DoD cyberspace career. To highlight these unique opportunities, DoD will:
    - Establish DoD as an employer of choice through coordinated campaigns designed to attract and inform potential candidates of the cyberspace opportunities at DoD
    - Review existing incentive programs for cyberspace talent in critical work roles and expand where needed, to include elements such as financial compensation, retention and skills-based proficiency bonuses, recognition, professional development and education programs

[7] The Associated Press, "Britain Eases Physical Standards for Military Cyber-Reservists," July 3, 2013.

- Augment recruitment efforts, as needed, with cyberspace subject matter experts for the purposes of identifying and attracting external candidates for cyberspace work roles

- **Foster non-traditional hiring for niche mission needs.** The Department seeks to attract highly skilled individuals who might otherwise be uninterested in regular government service. This may include world-class experts identified from competitions and games, as well as security conferences. To expand the pool of qualified candidates from formerly non-traditional areas of employment, the Department will:
  - Look beyond traditional hiring mechanisms, and consider other means such as part time or temporary work for specific missions as well as positions and programs for Highly Qualified Experts (HQEs), and Intergovernmental Personnel Act (IPA) assignments
  - Explore development of a focused set of authorities and processes that support employment of highly skilled personnel to address cyberspace mission requirements. This includes short term or temporary employment for personnel with the unique skills and knowledge needed for highly specialized tasks.

Focus Area 3: Institutionalize continuous learning with greater focus on evaluating the maturity of skills

> "*Too much of DoD's required cyber training is a static, check-the-box drill. DoD needs to develop a training program with evolving content that reflects the changing threat, increases individual knowledge, and continually reinforces policy.*"
>
> – DSB Task Force Report: *Resilient Military Systems and Advanced Cyber Threat*, January 2013

Education, classroom training and professional certification by themselves are insufficient to prepare personnel for rapidly changing cyberspace environments and threats. In many instances, experience and practicum is needed for obtaining and maintaining qualifications for cyberspace work roles. In order to support the diverse professional development requirements, the DoD cyberspace workforce will need an integrated learning continuum that provides a variety of training environments, including traditional classroom training; virtual training; hands-on laboratories; and realistic, operational exercises. Given the rapid changes in technology and proliferating threats, cyberspace personnel will require continuous learning that can be either broad or deep depending on their work role. To accommodate the complexity and criticality of these diverse needs, the Department will look to improve training effectiveness and efficiency by coherently managing cyberspace training requirements and standards, leveraging existing resources by employing a common set of training modules, where feasible, and utilizing DoD cyber-ranges.

Critical elements to institutionalize continuous learning for technical, non-technical, and leadership work roles are:

- **Manage cyberspace training standards and requirements.** The DoD Cyberspace Training Advisory Council (CyTAC) was established to identify, review, and assess training requirements and standards for currency and relevance to the contemporary cyberspace workforce. DoD components will continue to be responsible for developing training per established standards, as well as evaluating training effectiveness. Effectiveness of the training will be measured by an individual's ability to meet qualification requirements, at the unit or

organization-level through operational metrics and exercises; and, at the command-level by assessment of operational readiness.

- **Institute proficiency development and measurement.** Most technical and potentially some non-technical work roles require both knowledge and practical hands-on experience in order to mature skills. The Department will conduct an analysis of the DoD CWF to identify those work roles best suited for evaluating the maturity of an individual's skills. DoD will research and develop mechanisms to best measure proficiency for selected work roles and establish proficiency requirements by work role. Proficiency guidelines will then be coordinated throughout the Department and published in DoD issuances.
- **Identify and leverage Department-wide training and education opportunities.** DoD will establish an integrated learning continuum that comprises training, education, experience, and self-improvement. Currently, there are many training and education opportunities offered through various DoD organizations. To maximize investments, training and education opportunities that align with the DoD CWF work roles and qualifications will be identified from across the Department. These opportunities will include but are not limited to the DoD-funded Federal Virtual Training Environment (FedVTE), Defense Information Systems Agency (DISA) Information Assurance Support Environment (IASE) training products, courses from the Service Academies, National Defense University (NDU), iCollege, the Naval Postgraduate School, Air Force Institute of Technology, Defense Acquisition University (DAU), and other organizational programs external to the Department, such as Federally Funded Research and Development Centers (FFRDCs) and University Affiliated Research Centers (UARCs) offerings and best practices institutions. Since traditional classroom training is expensive, takes time away from the job and often involves travel time and money, development of alternative opportunities to enable remote, self-paced and mobile training will be integrated with more traditional opportunities.
- **Expand cyberspace learning requirements to all Department leaders.** It is imperative to advance the understanding of the role of cyberspace within the holistic DoD mission for both military and civilian leaders. All leaders need to be educated, trained, and experienced in cyberspace subject matter to enhance the warfighting capability of the United States through a heightened awareness of cyberspace requirements and capabilities. The Department will integrate cyberspace learning requirements into DoD civilian leadership development programs,[8] using cross-functional cyberspace learning requirements in military leadership development programs as a model.[9]
- **Establish an environment fostering continuous learning and professional development.** While the DoD CWF will provide the framework and lexicon of work roles with required knowledge, skills, and abilities, DoD issuances will outline qualifications, credentialing, and professional development requirements for each work role. The Department will cultivate a variety of opportunities to satisfy these requirements, including skill-based training, mission-based activities, exercises based on real-world use cases (e.g., table-top, capture the flag, war game, continuity of operations, command post and full-force exercises), and the evaluation of skills (as individuals, sub-teams, and holistically as a team). Continuous learning needs to include threat-based elements (e.g., based on evolving adversary tactics, techniques and procedures (TTPs)) enabling operations and engineering staff to understand adversary TTPs, since they must operate and engineer to counter those TTPs.

[8] Department of Defense Instruction (DoDI) 1430.16 – Growing Civilian Leaders
[9] Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 1800.01D – Officer Professional Military Education Policy

Additionally, all cyberspace staff needs some degree of threat-based cybersecurity training to most effectively perform in their work roles.

- **Provide for individual and collective training in a realistic and persistent simulated environment.** The Department has made a substantial investment in cyber-ranges. These ranges are capable of conducting a wide variety of tests, experimentation, and exercises to improve and assess cyberspace tradecraft and skills. These ranges will be leveraged to provide advanced, professional training and testing for individual and team development in an environment that can simulate realistic conditions, generate data, record data and results, and measure outcomes, while ensuring activities cannot be observed by adversaries.
- **Incentivize development of specialized training.** Niche skills are often needed for certain cyberspace missions, yet the focused training is not available. These might be skills in deeply specialized topics (e.g., cyberspace planning) or areas unique to a mission. The DoD will consider incentivizing Department subject matter experts who currently possess these niche skills to develop such courses by providing seed funding and will support the sharing of such courseware across the community. Additionally, as addressed in Focus Area 4, this advanced training can be used as a tool to retain personnel.

Focus Area 4: Retain qualified personnel

Today, the Department finds itself in competition with other government agencies and the private sector for highly qualified cyberspace personnel. While the private sector can generally offer higher compensation and benefits, the DoD offers opportunities and experiences that may attract some of the best and brightest by providing the environment and unique missions to retain cyberspace workers. If the Department can succeed here, recruiting becomes less challenging, since high-retention environments attract personnel.

Critical elements to retain qualified cyberspace performers are:

- **Provide career progression and meaningful challenges.** Throughout all types of organizations, a critical element in high retention rates is the ability of the organization to clearly show defined career progression opportunities, and offer meaningful and challenging work. To initiate the development of career progression criteria within the cyberspace workforce that will provide opportunities for cyberspace professionals to advance and develop, the Department and DoD components will map the DoD CWF to current function codes, military occupation codes and OPM occupational series for civilians. DoD components will map DoD CWF specialty codes to military and civilian positions and personnel. By mapping the DoD CWF to occupation codes, positions and personnel, DoD components can ensure cyberspace professionals are assigned to cyberspace-related positions throughout their career. While some cyberspace work roles will follow a prescribed career path, others will offer dynamic, non-linear career progression to broaden understanding of DoD missions and operations while applying cyberspace experiences and knowledge.
- **Offer training opportunities tied to retention commitments.** Along with meaningful and challenging work, many cyberspace professionals place a high value on specialized training and certification opportunities as outlined in Focus Area 3. These training opportunities can be costly, and in some instances, unavailable in a non-DoD setting. Offering training and certification, as part of retention commitments for both military and civilians, will show DoD interest in developing these personnel, as well as encouraging professional growth.

- **Retain qualified performers through compensation programs.** Retention or re-enlistment bonuses, as well as special and incentive pay often costs less than recruiting and training new employees (military and civilians). During the last decade, operational need focused on critical personnel such as medical doctors, nurses, pilots, nuclear propulsion engineers, and special operations personnel. While there is still focus in many of those areas, DoD must now also examine the operational need and criticality of the work roles within the cyberspace workforce, and develop comprehensive compensation programs to retain personnel with critical skills.
- **Identify and retain cyberspace leaders.** The Services currently have programs in place to develop well-rounded leaders. Expanding these types of programs to develop DoD civilians is vital for retaining skilled personnel that can lead the cyberspace workforce into the future. Leaders within the cyberspace workforce will be identified at multiple points throughout the career progression lifecycle and offered opportunities for individual and group mentoring, non-technical training to enhance leadership, and professional development, as well as rotational assignments (e.g., the Information Technology Exchange Program (ITEP)) to broaden technical and organizational knowledge. The ITEP program allows DoD and industry to experience the challenges each other face in management of their IT acquisitions, infrastructure and security requirements and exchange best practices on these issues.

Focus Area 5: Expand cyberspace threat knowledge

The increasing sophistication and frequency of threats targeting DoD, as well as the continual expansion of the more generalized threats that come from actively participating in cyberspace, requires the cyberspace workforce to increase awareness of the threat landscape. Current annual training requirements are a strong start to informing the workforce of the risks inherent in cyberspace; however, a single annual course is not enough to keep pace with the rapid changes in this domain. The Department must ensure the cyberspace workforce (civilians, military and contract support) have the knowledge needed to make responsible decisions when working in cyberspace.

Critical elements to expanding cyberspace awareness are:

- **Institute a cyber-threat knowledge program across DoD.** The Department will develop a cyber-threat knowledge training program at appropriate classification levels for all DoD personnel. Separate training will also be developed for targeted audiences requiring more specific knowledge, based upon their work roles. On a recurring basis, and as necessary, DoD personnel will participate in training and education sessions addressing current cyberspace threats, actors, activities, and impacts. Sessions will include content addressing individual responsibilities. These sessions may take the form of an online education, classroom interaction, or briefing. The material should be able to address both unclassified and classified environments. This training and education will be an ongoing program ensuring that all DoD personnel are knowledgeable of current and potential threats and activities; and may either replace or augment the current annual Information Assurance (IA) awareness training.
- **Establish standards and methods for individual reporting of potential cyberspace events.** Current IA training informs the workforce to contact their security officer in the event of certain suspicious activities; however, implementation and response varies across the Department (the user reporting procedures, the amount of information provided, and reconciliation actions). Therefore, DoD will develop a coordinated plan for encouraging and engaging the workforce to identify and report suspicious cyberspace activity in a standardized

method. Simple actions such as creating an email address and phone number, placing stickers with contact information on electronic devices to use for reporting suspicious activity, and employing more ongoing and consistent awareness campaigns will drive home the message of the importance of cyberspace awareness and response.

- **Test and evaluate cyber-threat awareness.** In order to determine the effectiveness of cyberspace threat awareness, the Department will increase the number of user training events, such as those addressing spear phishing. The intent of these events will be to assess workforce response and reporting choices throughout the year, as well as provide focused feedback to the participants to increase appropriate actions. User training events will increase in complexity as the workforce becomes more proficient in identifying and responding to suspicious activity, with metrics tracked at various levels throughout the Department.

Focus Area 6: Understand crisis and surge requirements and options

In cyberspace, any spot on the globe is seconds away. This virtual proximity simplifies the Department providing crisis or surge capabilities or capacity when highly specialized skills or extra staff is needed in cases such as a major incident at a unit that has insufficient resources to respond. However, a current limitation is lack of insight into the requirements and options for providing cyber-skilled personnel in a crisis. As part of conducting a mission analysis, the Department needs to consider how it could best leverage the cyber skills of the Reserve, National Guard, and DoD Civilians. If mission analysis indicates that organic skills and capacity are insufficient for surge support, DoD can examine options for leveraging personnel within the Defense Industrial Base (DIB) and other parts of the private sector.

Critical elements to understanding crisis and surge requirements and options are:

- **Analyze Reserve and National Guard support for cyberspace missions.** Currently, both the Reserves and National Guard have trained and qualified forces engaged in cyberspace missions. The citizen-soldiers of the National Guard and the Reserve offer DoD access to private sector cyber expertise within existing force structure. Initially, the Department can conduct a capacity and requirements analysis of crisis and surge capabilities necessary for conducting cyberspace missions. Then it can review sufficiency of in-house capacity and expertise to determine how best to draw upon the men and women of the National Guard and Reserve. DoD will continue to work with, the States and Federal partners, such as the Department of Homeland Security (DHS), to identify appropriate synergies.
- **Explore options to leverage DoD civilians with cyber expertise.** If mission analyses indicate that currently assigned DoD cyber personnel are insufficient for crisis or surge requirements, the Department could leverage existing DoD civilian staff. The Department can identify requirements for developing a DoD Civilian cyber-surge capability to identify qualified staff available from the broader DoD civilian workforce to address cyber-crises.
- **Identify options for accessing DIB sector cyber expertise.** Sharing of information between the DoD and the Defense Industrial Base was an important step in addressing widespread cyber-threats. This collaboration could expand to include sharing of DIB cyber personnel with the skills and clearances needed by DoD in a crisis. Additional mission analysis could assess whether this sharing could be reversed to provide a surge of DoD personnel to support DIB partners. Either option would require voluntary agreements or appropriate contract language.

- Any such collaboration must recognize that certain tasks may be inherently governmental or military essential functions, and that appropriate government control and oversight must be exercised at all times during cyber-crisis responses to ensure accountability, and protect against conflicts of interests or ethics concerns with the DIB.

- **Investigate options for accessing cyber expertise from other Public-Private partners.** In addition to evaluating options to leverage DIB personnel, the Department, in conjunction with DHS, could investigate mechanisms to appropriately tap into other expertise resident in the private sector. As with the DIB sector, such mechanisms must consider legal, regulatory, privacy, financial, training, eligibility and execution criteria.
    - Public-private partnerships must recognize that certain tasks will be inherently governmental or military essential functions, and that appropriate government control and oversight must be exercised at all times during cyber-crisis responses to ensure accountability, and protect against conflicts of interests or ethics concerns with the private sector partners.

Conclusion

While much progress has been made to date, there is still more to do. As General Alexander stated in his testimony on 27 March 2013, "Our progress, however, can only continue if we are able to fulfill our urgent requirement for sufficient trained, certified, and ready forces to defend U.S. national interests in cyberspace."[10]

This strategy document sets forth six strategic focus areas, providing the framework for DoD to meet current and future cyberspace workforce needs. Nothing in this strategy will subsume or replace the responsibilities, functions, or authorities of the heads of the DoD Components or other OSD officials as prescribed by law, assigned in chartering DoD directives, or detailed in other DoD policy issuances.

Emphasizing the commitment to DoD components, an implementation plan for the DoD Cyberspace Workforce Strategy will be developed to identify leads for each of the critical elements, follow-on actions, critical dependencies, roles and responsibilities of stakeholders as well as an annex addressing preface of cyberspace workforce management guidelines.

Executing these next steps will require:

- A commitment to continued and increased cooperation and collaboration across the cyberspace community.
- Identification of current and planned DoD initiatives that contribute to achieving the objectives.
- Alignment of cyberspace workforce policy, recruiting, training and retention efforts across the DoD.

[10] Statement of General Keith B. Alexander, Commander, United States Cyber Command before the Senate Committee on Armed Services, 27 March 2013. www.armed-services.senate.gov