Files\\2011 Case Study\\CS1\_Primary Sources\_Policy\_Strategies\\2010 Quadrennial Defense Review - § 6 references coded [ 0.24% Coverage]

Reference 1 - 0.01% Coverage

Develop greater cyber expertise and awareness;

Reference 2 - 0.02% Coverage

the QDR has elevated the need to preserve and enhance the AllVolunteer Force and included this priority in our force planning and in our strategy

Reference 3 - 0.06% Coverage

Recruiting and retention: Our recruiting efforts are long-term investments that can yield generational gains. In this challenging wartime environment, the Department continues to meet its recruiting and retention goals. The Department must continue developing innovative programs to attract qualified young men and women into the Armed Forces, and to retain them.

Reference 4 - 0.05% Coverage

 Revising bonus policies to allow the Military Departments to pursue innovative ways to retain quality personnel; and   
 Offering more flexible ways for military personnel to serve, by implementing programs designed to better enable transitions between Active and Reserve Component service.

Reference 5 - 0.04% Coverage

Developing future military leaders: The Department will continue its work to ensure that America’s cadre of commissioned and noncommissioned officers are prepared for the full range of complex missions that the future security environment will demand.

Reference 6 - 0.06% Coverage

Examples of efforts in this area include:   
 Building expertise in foreign language, regional, and cultural skills;  Recognizing joint experience whenever and wherever it occurs in an officer’s career; and  Ensuring that the Department’s educational institutions have the right resources and faculty that can help prepare the next generation of military leaders.

Files\\2011 Case Study\\CS1\_Primary Sources\_Policy\_Strategies\\2011 DoD Cyber Strategy - § 10 references coded [ 4.13% Coverage]

Reference 1 - 0.26% Coverage

The quality of the United States’ human capital and knowledge base in both the public and private sectors provides DoD with a strong foundation on which to build current and future cyber capabilities.

Reference 2 - 0.09% Coverage

Manage cyberspace risk through efforts such as increased training

Reference 3 - 0.46% Coverage

Co-location and dual-hatting of these separate and distinct   
Given its need to ensure the ability to operate Department of Defense Strategy for Operating in Cyberspace 5   
organizations allow DoD, and the U.S. government, to maximize talent and capabilities, leverage respective authorities, and operate more effectively to achieve DoD’s mission.

Reference 4 - 0.17% Coverage

This   
cultural shift will be enabled by new policies, new methods of personnel training, and innovative workforce communications.

Reference 5 - 0.16% Coverage

DoD will leverage the nation’s ingenuity through an exceptional cyber workforce and rapid technological innovation.

Reference 6 - 0.40% Coverage

The defense of U.S. national security interests in cyberspace depends on the talent and ingenuity of the American people. DoD will catalyze U.S. scientific, academic, and economic resources to build a pool of talented civilian and military personnel to operate in cyberspace and achieve DoD objectives.

Reference 7 - 0.45% Coverage

The development and retention of an exceptional cyber workforce is central to DoD’s strategic success in cyberspace and each of the strategic initiatives outlined in this strategy. DoD will assess its cyber workforce, requirements, and capabilities on a regular basis. The development of the cyber workforce is of paramount importance to DoD.

Reference 8 - 1.00% Coverage

The demand for new cyber personnel is high, commensurate with the severity of cyber threats. DoD must make itself competitive if it is to attract technically   
skilled personnel to join government   
service for the long-term. To achieve its objectives, DoD will focus on the establishment of dynamic programs to attract talent early, and the Department will leverage the 2010 Presidential Initiative to improve federal recruitment and hiring processes. DoD will also work with the Executive Office of the President to explore strategies designed to streamline hiring practices for its cyber workforce and exchange programs to allow for “no penalty” cross-flow of cyber professionals between the public and private sectors to retain and grow innovative cyber talent.

Reference 9 - 0.98% Coverage

Beyond these recruiting, education, and training initiatives, adoption and scaling of crossgenerational mentoring programs will allow DoD to grow a gifted cyber talent base for future defense and national security missions. Paradigm-shifting approaches such as the development of Reserve and National Guard cyber capabilities can build greater capacity, expertise, and flexibility across DoD, federal, state, and private sector activities. Opportunities for exchanges and continuing education programs will be explored by DoD, infusing an entrepreneurial approach in cyber workforce development. Continued education and training will be hallmarks of the cyber workforce, preserving, and developing DoD’s intellectual capital.

Reference 10 - 0.17% Coverage

DoD will invest in future personnel and capabilities to achieve its cyberspace objectives and support U.S. national security.

Files\\2011 Case Study\\CS1\_Primary Sources\_Policy\_Strategies\\2011 National Military Strategy - § 3 references coded [ 0.46% Coverage]

Reference 1 - 0.19% Coverage

To shape the future force, we must grow leaders who can truly out-think and out innovate adversaries while gaining trust, understanding, and cooperation from our partners in an ever-more complex and dynamic environment.

Reference 2 - 0.21% Coverage

The enduring challenges we face and the whole-of-nation approaches they require demand leaders that have the qualities of flexibility, agility, and adaptability, and the ability to build unique teams of teams to accomplish missions.

Reference 3 - 0.06% Coverage

we will maintain a whole, Joint Force that retains quality people,

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2014 Quadrennial Defense Review - § 3 references coded [ 0.15% Coverage]

Reference 1 - 0.02% Coverage

We will protect the health of the All-Volunteer Force as we undertake these reforms.

Reference 2 - 0.02% Coverage

MAINTAINING THE STRENGTH OF THE ALL-VOLUNTEER FORCE AND IMPLEMENTING NEW REFORMS

Reference 3 - 0.11% Coverage

As we restore balance to the Joint Force and the Department, the United States will maintain its two-fold sacred contract with U.S. Service members: to properly compensate and care for our men and women in uniform and their families both during and after their service, and to provide our Service members the best training and equipment possible so they can safely accomplish their missions.

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2015 DoD Cyber Strategy - § 11 references coded [ 2.21% Coverage]

Reference 1 - 0.15% Coverage

This strategy builds on previous decisions regarding DoD’s Cyber Mission Force and cyber workforce development and provides new and specific guidance to mitigate anticipated risks and capture opportunities to strengthen U.S. national security.

Reference 2 - 0.18% Coverage

DoD will focus on ensuring that its forces are trained and ready to operate using the capabilities and architectures they need to conduct cyber operations, continue to build policy and legal frameworks to govern CMF employment, and integrate the CMF into DoD’s overall planning and force development.

Reference 3 - 0.19% Coverage

In 2013 DoD initiated a major investment in its cyber personnel and technologies by initiating the CMF; now DoD must make good on that investment by training its people, building effective organizations and command and control systems, and fully developing the capabilities that DoD requires to operate in cyberspace.

Reference 4 - 0.25% Coverage

Build the cyber workforce. To make good on DoD’s significant investment in cyber personnel, and to help achieve many of the objectives in this strategy, DoD’s first priority is to develop a ready Cyber Mission Force and associated cyber workforce. This workforce will be built on three foundational pillars: enhanced training; improved military and civilian recruitment and retention; and stronger private sector support.

Reference 5 - 0.12% Coverage

Maintain a persistent training environment. DoD requires an individual and collective training capability to achieve the goals outlined in this strategy and to meet future operational requirements.

Reference 6 - 0.13% Coverage

Build viable career paths. Throughout the course of this strategy, and following the CMF decisions of 2013, DoD will continue to foster viable career paths for all military personnel performing and supporting cyber operations.

Reference 7 - 0.27% Coverage

Draw on the National Guard and Reserve. Throughout the course of this strategy, DoD will draw on the National Guard and Reserve Components as a resource for expertise and to foster creative solutions to cybersecurity problems. The Reserve Component offers a unique capability for supporting each of DoD’s missions, including for engaging the defense industrial base and the commercial sector. It represents DoD’s critical surge capacity for cyber responders.

Reference 8 - 0.24% Coverage

Improve civilian recruitment and retention. In addition to developing highly-skilled military personnel, DoD must recruit and retain highly-skilled civilian personnel, including technical personnel for its total cyber workforce. Civilians must follow a welldeveloped career development and advancement track and be provided with best-inclass opportunities to develop and succeed within the workforce.

Reference 9 - 0.33% Coverage

Develop and implement exchange programs with the private sector. To supplement DoD’s civilian cyber workforce, DoD must be able to employ technical subject matter experts from the best cybersecurity and information technology companies in the country to perform unique engineering and analytic roles within DoD. The Defense Department will implement successful private sector exchange programs to bring measurable benefits to the Department of Defense through the design and development of new operational concepts for DoD’s cyberspace missions.

Reference 10 - 0.26% Coverage

Support the National Initiative for Cyberspace Education. DoD will develop policies to support the National Initiative for Cybersecurity Education. Working with interagency partners, one or more educational institutions, as well as state and private sector partners, DoD will continue to support innovative workforce development partnerships focused on both the technical and policy dimensions of cybersecurity and cyber defense.

Reference 11 - 0.09% Coverage

As always, our women and men – both uniformed and civilian personnel – will be our greatest and most enduring strength and a constant source of inspiration.

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2015 National Military Strategy - § 10 references coded [ 2.79% Coverage]

Reference 1 - 0.16% Coverage

It echoes previous documents in noting the imperative within our profession to develop leaders of competence, character, and consequence.

Reference 2 - 0.30% Coverage

Despite what is likely to be a difficult future, we are blessed to be able to count on the   
young Americans who choose to serve, to live an uncommon life, and to defend their fellow citizens. Our focus must remain that they are the best-led and best-equipped force in the world.

Reference 3 - 0.44% Coverage

A. People and the Profession of Arms: Improving Upon Our Greatest Advantage Our military and civilian professionals are our decisive advantage. They are the   
foundation of our operational excellence and our ability to successfully innovate. Therefore, we are dedicated to building creative, adaptive professionals skilled at leading organizational change while operating in complexity.

Reference 4 - 0.04% Coverage

Producing creative, adaptive leaders

Reference 5 - 0.29% Coverage

We must prepare our Service members to fight under conditions of complexity and persistent danger, conditions that demand courage, toughness, adaptability, and endurance as well as an abiding commitment to our Nation’s values and professional military ethic.

Reference 6 - 0.31% Coverage

We are prioritizing leader development. To retain our warfighting edge, we are stressing innovative leader development across the All-Volunteer Force — officer, enlisted,   
13   
and civilian — through a combination of training, education, broad experience, and opportunity.

Reference 7 - 0.94% Coverage

Our military education system also is updating how it selects and incentivizes faculty, rewards critical thought, and promotes our most innovative minds. Continuous, demanding education inspires new ideas and identifies better ways to accomplish our missions.   
In developing the Joint leaders of tomorrow, we emphasize six attributes. Our leaders will:   
 Strive to understand the environment in which they operate and the effect of applying all instruments of national power   
 Anticipate and adapt to surprise, uncertainty, and chaos  Work to recognize change and lead transitions  Operate on intent through trust, empowerment, and understanding  Make ethical decisions based on the shared values of the Profession of Arms  Think critically and strategically in applying joint warfighting principles and concepts to joint operations

Reference 8 - 0.12% Coverage

To enhance our warfighting capability,   
we must attract, develop, and retain the right people at every echelon.

Reference 9 - 0.14% Coverage

the U.S. military must be willing to embrace social and cultural change to better identify, cultivate, and reward such talent.

Reference 10 - 0.04% Coverage

We are promoting ethical leadership.

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2015 National Security Strategy - § 2 references coded [ 0.11% Coverage]

Reference 1 - 0.03% Coverage

promoting talent and diversity in our national security workforce

Reference 2 - 0.08% Coverage

Above all, we will take care of our people. We will recruit and retain the best talent while developing leaders committed to an ethical and expert profession of arms.

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2015 White House Report on Cyber Deterrence Policy - § 1 reference coded [ 0.29% Coverage]

Reference 1 - 0.29% Coverage

The Administration seeks to shape the future of cybersecurity through a comprehensive plan and investment strategy to develop the tools, techniques, and national workforce necessary to continue to improve the resilience of U.S. computers, networks, and critical infrastructure and provide new technological options for deterring malicious cyber activities.

Files\\2018 Case Study\\CS3\_Primary Sources\_Policy\_Strategies\\2018 National Cyber Strategy - § 5 references coded [ 1.05% Coverage]

Reference 1 - 0.24% Coverage

Develop a Superior Cybersecurity Workforce   
A highly skilled cybersecurity workforce is a strategic national security advantage. The United States will fully develop the vast American talent pool, while at the same time attracting the best and brightest among those abroad who share our values.

Reference 2 - 0.13% Coverage

The United States Government will continue to invest in and enhance programs that build the domestic talent pipeline, from primary through postsecondary education.

Reference 3 - 0.13% Coverage

The Administration will work with the Congress to promote and   
reinvigorate educational and training   
opportunities to develop a robust cybersecurity workforce.

Reference 4 - 0.30% Coverage

To improve recruitment and retention of highly qualified cybersecurity professionals to the Federal Government, the Administration will continue to use the National Initiative for Cybersecurity Education (NICE) Framework to support policies allowing for a standardized approach for identifying, hiring, developing, and retaining a talented cybersecurity workforce.

Reference 5 - 0.24% Coverage

The Administration will promote appropriate financial compensation for the United States Government workforce, as well as unique training and operational opportunities to effectively recruit and retain critical cybersecurity talent in light of the competitive private sector environment.