Software Engineering Institute

State of Cyber Workforce Development

Marie Baker

August 2013

WHITE PAPER

CERT Division

http://www.sei.cmu.edu

Carnegie Mellon

Table of Contents

1 Introduction 1

1.1 Purpose and Scope 2
1.2 Audience 2
1.3 Document Structure 2

2 Training Initiatives 3

2.1 Department of Defense (DoD) Directive 8570.01 Information Assurance Training, Certification, and Workforce Management 3
2.2 Department of Defense (DoD) Directive 8140 Cyberspace Work-Force Management Policy Update 3
2.3 USCYBERCOM Joint Cyberspace Training & Certification Standards (JCT&CS) Initiative 4
2.4 The National Initiative for Cybersecurity Education (NICE) 5
2.5 DHS's CyberSkills Task Force Report 6
2.6 The DISA Operationally Focused CYBER Training Framework 7
2.7 CERT Approach to Cybersecurity Workforce Development 8

3 Resources for Cyber Workforce Training and Development 10

3.1 National Centers of Academic Excellence 10
3.2 CyberCorps Scholarship for Service 10
3.3 Federal Virtual Training Environment 10
3.4 STEPfwd 11
3.5 State-Wide Initiatives 11

4 Next Steps 13

5 Conclusion 15

References 16

Executive Summary

Currently, the United States is arguably in a dire situation in terms of cyber preparedness. Cyber attacks and their sophistication are growing exponentially, while the cyber workforce is struggling to develop and sustain the talent needed to protect, detect, defend, and respond to these attacks. Since the nation has become deeply dependent on cyberspace, the realization of an attack is a risk with detrimental consequences to critical services and every sector.

In response to this crisis and the potential threat to U.S. security, several cyber workforce training and retention programs have been established to grow and retain a pool of highly skilled cyber professionals. These programs are described in this white paper, along with a survey of projects that support them and examples of initiatives designed to accelerate the growth of a talented cyber workforce. While these projects and initiatives offer training and development mechanisms designed to enhance the knowledge and skills of the cybersecurity workforce, there are gap areas that need to be addressed to achieve measurable success.

The *Next Steps* section summarizes these gap areas and presents strategies for training frameworks moving forward.

1 Introduction

Cyberspace is widely recognized as a global domain in the information environment. Critical services, resources, and operations are contingent on the availability and reliability of networked connectivity; however, being highly reliant on computer systems also means being highly vulnerable to devastation in the wake of a cyber attack.

An attack targeting a nuclear facility in recent years used a cyber weapon of unprecedented complexity and power, demonstrating the maturity of malicious code and its ability to impact the operations of an entire facility. This weapon, a worm named Stuxnet, has caused global concern since it can be copied and modified to be launched against other facilities, altering their operations or completely destroying them. According to an assessment presented to Congress in March 2013 by some of the nation's top intelligence officials, cyber attacks lead the list of security threats the United States faces.

In recent years, confidence in the nation's preparedness to handle a major cyber attack has been low. In a 2010 interview, James Gosler, a veteran cybersecurity specialist who has worked at several government agencies, warned that there is a lack of sufficiently bright people moving into fields that support national cybersecurity objectives. He surmised that there were 1,000 people in the U.S. with the skills required to undertake demanding cyber defense tasks. Gosler further estimated that to meet the needs of U.S. government agencies and corporations, the number of skilled cybersecurity professionals would need to grow to between 20,000 and 30,000.

Exacerbating this situation is the comparison of the U.S. to other countries, specifically China, in terms of cyber expertise. China has made training cybersecurity experts a high priority, and these focused efforts are having an impact. Chinese universities have historically dominated cyber competitions held by major corporations. According to Verizon's *Data Breach Investigation Report 2012*, in which researchers examined more than 47,000 security incidents that occurred in 2012, 21 percent of these incidents were carried out by state-affiliated hackers on espionage missions, 96 percent of which could be tracked back to China [Hamill 2013].

Because of an exploited vulnerability's crippling effect on the computer networks of critical infrastructure industries, great emphasis has been placed on having a well-trained cyber workforce that is prepared to perform defensive and offensive operations in cyberspace.

To support this *force readiness* effort, several cyber workforce development initiatives were established. These training initiatives reinforce U.S. Army General Keith Alexander's vision and strategic roadmap. General Alexander called for common, demanding standards that include individual and collective staff training as well as assessment of the trained staff's ability to perform a mission. He is quoted as saying

> *"Whether we do our cyber-training at one school or at multiple schools, the training will have to be executed to one standard. I think that's what we need to do so that the combatant commanders and the forces in the field know that whether they get a soldier, marine, airman or sailor, that person is trained to a standard and can accomplish the mission that is expected of them"* [USCC 2010].

This document highlights several cyber workforce development and retention plans, and details their approaches to support the goal of creating (through mission-specific training standards) a robust cybersecurity workforce that is prepared to protect and defend cyberspace.

1.1 Purpose and Scope

The purpose of this paper is to highlight the critical position the nation is in due to our profound dependence on cyberspace, the volume and sophistication of cyber attacks that threaten essential systems that rely on cyber networks, and the lack of skilled cyber professionals able to operate in cyberspace both offensively and defensively.

This paper also summarizes the current posture of the cyber workforce and several of the initiatives designed to strengthen, grow, and retain cybersecurity professionals.

1.2 Audience

The primary audience of this paper includes individuals with a stake in cybersecurity workforce development. Whether used by a manager of an organization with a significant cyber footprint, a leader in government or military sectors, or members of the cyber workforce investing in their future in cybersecurity operations, the information contained in this paper should serve as a resource for current activities, trends, and proposed strategies moving forward.

1.3 Document Structure

This document compares DoD and Federal civilian agency doctrine, goals, approaches, plans, and current activities in their cyber workforce development programs. The introduction presents specific examples and explanations of why cybersecurity is so concerning on a national level and why it's imperative to develop and retain a skilled cybersecurity workforce. Next, several training and development initiatives are described, followed by a survey of programs that support these initiatives as well as case studies that illustrate successful training approaches. The paper concludes with some observations about workforce development programs and areas that would benefit from additional focus moving forward.

2 Training Initiatives

2.1 Department of Defense (DoD) Directive 8570.01 Information Assurance Training, Certification, and Workforce Management

One of the first cyber workforce training initiatives established is the Department of Defense *(DoD) Directive 8570.01 Information Assurance Training, Certification, and Workforce Management* initiative. This initiative is designed to provide the basis for an enterprise-wide solution to train, qualify, and manage the DoD Information Assurance (IA) workforce. The directive calls for information assurance technicians (IAT) and managers (IAM) to be trained and qualified at a baseline requirement. The policy applies to all organizational entities in the DoD performing IA functions.

The manual that provides guidance and procedures for supporting the directive, DoD 8570.01 *M*, was approved in December 2005. The latest version, Change 3, was published in January 2012. The directive addresses workforce management issues by calling for IA positions to be identified and documented, and for qualified personnel to be identified and assigned to those positions.

To reach this goal, all IA positions are categorized as technical (IAT), management (IAM), system architecture and engineering (IASAE), or computer network defender service provider (CND SP) and are assigned a level or specialty within each category. Individuals must obtain an approved certification from a category to be qualified for a corresponding position. Change 3 specifies that all personnel who perform IA functions must obtain a baseline and computing environment certification and/or certificate of training within six months of being hired in an IA position.

The goal of *DoD 8570.01* is to build an IA workforce with the knowledge and skills to protect and defend DoD systems and information assets in cyberspace. The right people with the right skills will be in the right position. The office of the DoD Chief Information Officer (CIO) validates, monitors, and reports on the certification status of IA workforce members through the Defense Workforce Certification Application (DWCA) database.

2.2 Department of Defense (DoD) Directive 8140 Cyberspace Work-Force Management Policy Update

DoD 8140 Cyberspace Workforce Management Policy Update will replace *DoD 8570*. Expected to be published in January 2014, *DoD 8140* will provide a comprehensive view of the cybersecurity workforce; include law enforcement, intelligence, and Netops personnel; and change levels I, II, and III to *apprentice*, *journeyman*, and *master*.

Additional plans include an *Information Assurance Workforce Improvement Program* that captures the current workforce construct, and integrates job skills and functions from the National Initiative for Cybersecurity Education (NICE) framework, and mission area requirements from the U.S. Cyber Command (USCYBERCOM) workforce. The NICE and CYBERCOM initiatives are discussed later in this paper.

The goal of the *DoD 8140* is to maintain a comprehensive workforce management perspective that will result in a channel of qualified IA workforce personnel. Positions performing cyberspace functions will be documented in manpower systems, and workforce personnel qualifications will also be kept within records systems. Compliance with this policy will be included in DoD inspection programs.

2.3 CYBERCOM Joint Cyberspace Training & Certification Standards (JCT&CS) Initiative

USCYBERCOM has three Lines of Operations (LOOs) from which cyber forces must be trained and mission ready: Offensive Cyber Operations (OCO), Defensive Cyber Operations (DCO), and DoD GIG Operations (DGO). USCYBERCOM has directed its training and development efforts through the Joint Cyberspace Training & Certification Standards (JCT&CS) Initiative. The JCT&CS is the first joint cyber training framework of its kind. It is designed to be continuous, growing, and adapting as technologies and tactics evolve.

The objective of the JCT&CS initiative is to have forces trained and ready to meet the challenges of cyberspace. To reach this goal, the training program calls for creating common, arduous standards for both individuals and collectives, administering first-rate training, and accurately evaluating the forces' capabilities to perform missions. In support of General Alexander's statement, the initiative is designed to establish joint training and certification standards to achieve his end-state of a workforce that "can accomplish the mission that is expected of them."

The joint training and certification standards developed by the JCT&CS are in the operational context and mission requirements of CYBERCOM and its components. Training standards are defined for each job role and for collective audiences. The joint procedures and guidelines for implementing the initiative are patterned after the Joint Training System's (JTS's) four phases: requirements, planning, execution, and assessment. The JTS framework provides commanders with integrated processes used to evaluate the command's missions and to determine the tasks essential to accomplishing those missions. These processes are designed to improve the commander's joint readiness by linking plans, training, and assessment to mission requirements.

A prioritized list of essential tasks, their conditions, and measurable standards required to accomplish a mission are created. This list is known as the Joint Mission Essential Task List (JMETL). The JMETL helps to form the answer to the question of mission readiness: To complete this mission, this organization must accomplish these tasks under these conditions to meet these standards.

The ability to accomplish CYBERCOM missions starts with a baseline knowledge of cyberspace operations. Building on existing initiatives, CYBERCOM developed a list of cyber work roles that includes the tasks and skill sets required to perform the work role in the three LOOs. The tasks and skill sets establish this baseline. Proficiency ratings that reflect knowledge, skills, and abilities (KSAs) are correlated to training and job requirements. KSAs are measures that specify the level of task performance. Individuals must attain the minimum proficiencies required to complete a given work-role task.

Training plans that include audiences, objectives, and methods are identified based on the requirements defined in the JMETL and the baseline standards. The plans to achieve the requirements-based training objectives are executed, collecting feedback throughout as inputs for the assessment phase and planning for the next training cycle. The assessment phase completes the training cycle once the Training Proficiency Assessment (TPA) is completed. The TPA is a collection of inputs from Task Performance Observations (TPOs), Training Proficiency Evaluations (TPEs), and the observation of real-world operations. The TPAs and Mission Training Assessments (MTAs) are entered into the Joint Training Information Management System (JTIMS) where lessons learned are made available for the planning phase of the next training cycle.

2.4 The National Initiative for Cybersecurity Education (NICE)

The National Initiative for Cybersecurity Education (NICE) was established in response to the Comprehensive National Cybersecurity Initiative (CNCI), a published set of initiatives created to help secure the United States in cyberspace (specifically, CNCI Initiative 8 calls for the need to expand cyber education, awareness, and professional development). NICE has three goals and three target audiences.

The first goal is to raise the general public's awareness of the risks in cyberspace. The second is to broaden the pool of prepared cybersecurity workforce members and focuses on students. The third goal is to cultivate a globally competitive cybersecurity workforce. These goals are organized under components, each led by one or more federal agencies, and have defined objectives and strategies for meeting those objectives. For the purpose of this document, the focus will be on the third goal and its objectives.

Having the right people with the right skills at the right time and place (collectively known as *effective human capital planning*) is a need identified in the cybersecurity workforce to achieve global competitiveness. Because the cybersecurity industry is still evolving, many aspects of the field are not yet defined, and the knowledge and skills of the workforce are weak. NICE plans to achieve goal three by forming the foundation on which to build a robust and talented cyber workforce. This foundation will be built by establishing standards and strategies for training and career development, projecting human capital needs, and developing mechanisms for categorizing cybersecurity job roles.

The first objective of this goal is to develop and adopt the *National Cybersecurity Workforce Framework*. The framework, published in 2012, addresses the need for standard terminology, cyber workforce position descriptions, and required knowledge, skills, and abilities. Within the framework, categories and specialty areas are used to organize and group similar types of work. Categories serve as an overarching structure for the framework and group related specialty areas together. Each specialty area contains common tasks and KSAs. The framework is designed to define cybersecurity work regardless of organizational structure or job title yet be flexible enough to allow entities to adapt content to their workforce-planning needs.

The NICE initiative contains 7 categories and 31 specialty areas. The Office of Personnel Management (OPM) will issue codes corresponding to these categories and specialty areas. The codes will then be used to consistently identify the cyber workforce, determine a baseline of capabilities,

evaluate workforce demands, identify training gaps, and aid in the effective recruitment and retention of a skilled workforce.

The second objective of goal three is the development of tools for forecasting the cybersecurity workforce. These tools will collect data to examine the current cybersecurity competencies of the nation's workforce. That data will be used to create a baseline of the workforce's characteristics and for the research, development, and forecasting of future needs.

The third objective of goal three is the establishment of standards and guidance for cybersecurity training and professional development. Ongoing, specialized training is necessary to ensure the cyber workforce has the appropriate technical skills and resources needed to fulfill its role. This objective will be met using an online resource that provides cybersecurity professionals with information on training opportunities that align with the specialty areas in the NICE initiative. This online resource will also help identify gaps between specialty area needs and training opportunities. A void in training in a specialty area may add risks to the nation's cyber workforce readiness; identifying and creating a training plan for these gap areas will help mitigate those risks.

In February 2013, the U.S. Department of Homeland Security (DHS) launched a tool that supports the NICE effort (specifically the third objective). The National Initiative for Cybersecurity Careers and Studies (NICCS) is a comprehensive, publically available, online resource that contains cybersecurity education, training, and career information. The information is categorized and searchable using (among other criteria) specialty area and proficiency level.

The fourth and fifth objectives of the third goal are identifying best practices to help recruit and retain cybersecurity professionals, and evaluating the professionalization of the cybersecurity workforce. Both of these objectives are subjects of ongoing research strategies that share the end goal of providing best practices and other outcomes.

2.5 DHS's CyberSkills Task Force Report

Besides the previously mentioned online resource, DHS published the *CyberSkills Task Force Report, Fall 2012* [Homeland Security Advisory Council 2012]. The CyberSkills report is the result of the task force formed by DHS Secretary Janet Napolitano in response to the acknowledged urgency of the nation's need for trained professionals with the skills required to defend and respond to the volume and sophistication of recent cyber attacks. Napolitano said that cybersecurity is the most dynamic and threatening risk we face; she believes that by implementing the report's recommendations, federal agencies and private sector entities will have the skilled cybersecurity workforce required to achieve their mission of preventing, detecting, and responding to cyber attacks.

The formation of the Task Force on CyberSkills came with a two-part mandate:

1. Identify how DHS can best develop a cybersecurity workforce that is able to handle cybersecurity challenges.
2. Detail how DHS can recruit and retain that talent.

The report details how to meet the mandate and, if implemented as described, how it will increase the cybersecurity skills of the workforce and put DHS in the position of being its preferred employer. This skilled workforce will, in turn, aid in making the U.S. more secure and resilient.

The DHS Task Force on CyberSkills made 11 recommendations grouped under five objectives. One objective is to adopt and maintain an authoritative list of mission-critical cybersecurity tasks. The tasks identified in the *CyberSkills Task Force Report* represent the skill gaps that task force members believe are essential for DHS to fill to be the nation's nerve center for ensuring a secure and resilient infrastructure. This list of mission-critical jobs, their required tasks, and the consequences of failure to perform these tasks will be kept current and evolve in tandem with the shifting threat landscape.

The ten mission-critical skills listed in the report are defined for DHS-specific missions. However, to leverage the NICE framework and its catalog of tasks and skills, DHS will clarify functional roles in the framework, define DHS-specific job requirements, and prioritize and categorize these roles as mission-critical or non-mission-critical.

The remaining objectives to be met if the 11 recommendations are implemented include specific details for training, assessing skills, recruiting, and retaining employees with mission-critical cybersecurity skills. The final objective calls for the establishment of a CyberReserve program that will include DHS maintenance of a protected information inventory of individuals who have basic proficiency and mastery skill levels in each of the identified mission-critical skills. Having this valuable information allows DHS to quickly fill a specific job need and rapidly locate talent in the event of an emergency.

2.6 The DISA Operationally Focused CYBER Training Framework

The Field Security Operations office of the Defense Information Systems Agency (DISA) released the *Operationally Focused CYBER Training Framework* in spring 2012. The vision of this framework is similar to the other training initiatives that use a role-based training and assessment approach. Its goal is to better prepare the cybersecurity workforce through a robust training and certification program designed around the "one standard" concept from General Alexander's directive.

The basic tenets of DISA's plan include using a training strategy roadmap customized for role-based and crew certification through certifications based on mission-specific qualifications rather than broad commercial certifications. A crew certification is a composition of qualified role-based operators who attained the necessary skill sets to defend and operate in cyberspace. Role-based individuals are qualified to work as part of a crew through a Cyber Defense Academy. The DISA framework uses the JCT&CS for baseline work-role definitions and the NICE framework for baseline federal and DoD work-role definitions.

The implementation plan for DISA's role-based training and assessment begins with using the work roles defined by the JCT&CS and NICE framework and the roles' associated tasks and KSAs required to create a roles-and-tools training matrix. Depending on the mission, roles require tool and function training. Individuals within the roles will need further training on how to inter-

face with other roles and how their tools interface with others. This training is defined as tools and functions training that focuses on roles-to-tools, tools-to-tools, and roles-to-roles interactions.

DISA maintains a role-based curriculum website where users may locate training resources for specific roles. The information is organized by specialty. The trainee can locate the specific KSAs required for the tasks within a specialty role. The provider of training can use the website to meet those requirements. Future plans include mapping training to KSAs and using that mapping to create individual development plans (IDPs).

Looking ahead, DISA also plans to provide a tactics, techniques, and procedures (TTPs) template and repository to better organize and define the TTPs and the skill and role levels for tasks. DISA also plans to work on the foundation of a DoD Cyber Defense University Academy that, in coordination with education and operations leaders, will specialize in cyber role-based training and assessment products, as well as qualification standards.

2.7 CERT Approach to Cybersecurity Workforce Development

The CERT Division of the Carnegie Mellon® Software Engineering Institute (SEI), a federally funded research and development center sponsored by the U.S. Department of Defense, subscribes to workforce development divided into continuous phases of development. These phases progressively build an individual's knowledge, skills, and experience in ways that are relevant to his or her job duties. Three main phases are followed by an evaluation phase to assess the individual's comprehension of the training.

Phase 1, knowledge building, focuses on teaching fundamental skills and concepts to the learner. This teaching is typically done in a traditional instructor-led classroom; however, online deliveries are becoming increasingly more desirable due to cost-effectiveness and time efficiency.

Phase 2, skill building, reinforces concepts learned in the previous phase through task-focused, hands-on exercises. This phase is an integral part of professional development because individuals transform knowledge into the ability to apply it. These exercises focus on an individual skill and take place in a controlled environment free of distractions. Once individuals have accomplished those exercises, they can further refine their skills in the experience-building phase.

Phase 3, the experience-building phase, refines the knowledge and skills by applying them to real-world, on-the-job scenarios that lead to maximizing the individual's job performance. No longer in a controlled environment, these scenarios force individuals to successfully operate with additional complexities and unfamiliarity.

Phase 4, the evaluation phase, assesses the knowledge comprehension and skill proficiency achieved through the training. The assessment helps to determine the next training cycle for the individual and serves as a mechanism for organizations to better understand the workforce's strengths and additional training needs.

® Carnegie Mellon is a registered trademark of Carnegie Mellon University.

The CERT Division's approach using continuous phases of development progressively builds an individual's ability and leverages online platforms for knowledge, skills, and experience building. In the end, the approach offers organizations a comprehensive, targeted, and cost-effective training option that can be tailored to their needs [Hammerstein 2010]. Two specific online platforms developed by the CERT Division support this approach and are currently being used by the federal cyber workforce: FedVTE for knowledge and skill building, and STEPfwd (formerly XNET) for experience and evaluation. These platforms are discussed later in this paper.

3 Resources for Cyber Workforce Training and Development

In recent years, several cybersecurity training and workforce development initiatives were established that support the directives and frameworks outlined previously, and contribute to the advancement of the cybersecurity workforce. The following is a survey of some of these programs and initiatives, and the audiences they target.

3.1 National Centers of Academic Excellence

Another program from DHS, jointly sponsored with the National Security Agency (NSA), is the *National Centers for Academic Excellence in IA Education, Education and Training, and IA Research*. These centers, totaling 166 in 2012, are higher education institutions that were recognized as leaders in these fields. Graduates from these programs often become cyber experts who have the ability to protect and defend national information infrastructures. The goal of the program is to promote IA disciplines and produce a growing number of trained IA professionals. The list of Centers of Academic Excellence (CAE) institutions and the programs they offer is available on the NSA website.

3.2 CyberCorps Scholarship for Service

The CyberCorps Scholarship for Service (SFS) program was established to help the federal government recruit, train, and retain skilled cybersecurity professionals who are qualified to defend and protect critical services. The program provides scholarships to eligible college students to fully cover the cost (including boarding, books, and stipends) of an approved higher education institution. In return, upon graduation the grant recipient commits to an internship and later employment at a government organization for a period equal to the length of their scholarship benefits. The SFS program is managed by the U.S. Office of Personnel Management with scholarships funded through grants awarded by the National Science Foundation (NSF).

The SFS program has a graduation rate of 150 to 160 students per year, and the program continues to grow. A $30 million dollar budget increase for the program was recently received, taking the budget from $15 million in 2011 to $45 million in 2012 [Roman 2012].

3.3 Federal Virtual Training Environment

The Federal Virtual Training Environment (FedVTE) is an online training and learning management system managed by DHS with support from DISA and the U.S. Department of State. In 2005, the SEI developed a virtual training environment (VTE) to address DoD training and capability-building challenges related to information security. In 2012, VTE was redesigned with enhanced features to better meet cyber workforce training requirements and made the transition to FedVTE to serve federal employees.

Due to the highly mobile nature of the DoD workforce, existing classroom-based training solutions failed to adequately prepare students to manage and defend government networks. The SEI converted recorded classroom instruction into an online format allowing students around the

globe to access training material on their own time. The training materials include IA and topical cybersecurity courses, complete with reinforcing video demonstrations, hands-on labs where students employ lessons learned in a virtual environment, and quizzes for comprehension assessment. FedVTE is an example of a tool that can be used to follow the CERT Division's approach of development in phases of knowledge, skills, and experience building.

FedVTE serves tens of thousands of government and military users, and over 30,000 hours of training materials are accessed per month. This system saves millions of dollars in travel and training costs because Federal cybersecurity professionals can access it free of charge from anywhere in the world.

3.4 STEPfwd

STEPfwd incorporates features previously available in the CERT Division's exercise network, XNET. These features include network simulations ranging from just a few servers to thousands of network nodes. STEPfwd supports the experience and evaluation phase of the CERT workforce development approach through its hands-on training platform and performance assessment data. The STEPfwd exercise network is an isolated environment that can host hundreds of systems and associated networking that simulates a real-world environment. All aspects of training exercises can be customized to replicate operational networks. STEPfwd exercises feature the added realism of functional versions of popular internet sites and a first-of-its-kind user simulator and helpdesk ticketing system that replicates typical traffic users generate, and tests that confirm enterprise service availability.

The U.S. Cyber Command (USCC) Exercise Network is the USCC's customized instantiation of XNET that was developed in partnership with the SEI. This exercise network was the largest and most realistic ever developed for military cyber training. In addition to the operational realism created, in part, with over 7,500 virtual servers, real-time status and post-mortem exercise analysis were also available for exercise administrators. USCC's XNET is used in large organized military cyber defensive training events such as CYBER FLAG and Cyber Guard.

In a March 2012 statement before the House Committee on Armed Services Subcommittee on Emerging Threats and Capabilities, USCC Commander and Army General Keith Alexander spoke of the USCC's first major tactical exercise called CYBER FLAG. The large, multi-day event put operators in engaging, realistic, simulated, cyber-combat exercises. While the event attracted a great deal of attention, according to General Alexander, the CYBER FLAG exercise is not seen as a mere drill; the lessons learned first-hand are applied daily in defense of networks.

3.5 State-Wide Initiatives

Several states (most newsworthy lately, Florida, Maryland, and Texas) have taken on cyber operations at the state level. State and local governments partnered with universities and public and private industries to establish cybersecurity awareness and development programs. In addition to resources that offer education and awareness information on cyber crime and attacks for their citizens, these states are dedicating resources to position themselves to be leaders in the cybersecurity industry.

The state of Texas invested in a holistic approach to improving the infrastructure of cybersecurity operations and education, and several ways to position the state for accelerated growth in the cybersecurity industry. In 2011, the governor of Texas signed a bill authorizing the creation of the Texas Cybersecurity, Education, and Economic Development Council. The council members—representatives of government, academia and industry—analyzed the existing cyber posture of the state of Texas and prepared a report of their findings and suggestions in 2012.

The council found that Texas already had many strengths that would contribute to making the state a cybersecurity industry leader; a framework to align these strengths together is where future efforts will be applied. One of the strengths is the success of San Antonio's model of collaboration with local government, military, universities, local schools, and businesses to increase cybersecurity education and awareness. Besides having 3 of Texas's 12 NSA/DHS Centers of Academic Excellence in Information Assurance located in San Antonio, the city has 60,000 technology workers and is home to the nation's largest military installation with nearly 80,000 DoD personnel [CyberCityUSA.org 2013]. With these large populations representing every sector collaborating on cybersecurity education and initiatives, the city once known as "Military City, USA" is transitioning to "Cyber City, USA."

The education of Texans starts young. Cyber awareness curriculum for K-5 students is being implemented and will continue through high school where additional cyber-focused programs are available. The Alamo Academies, a program for Texas high-school students, was created through a partnership of industry, local government, public school systems, and community colleges. This program gives high-school juniors and seniors an opportunity to prepare for future employment by taking college-level courses and participating in summer internships. The goal of the Alamo Academies is to expose students earlier to cyber-related studies and accelerate the learning of potential future cyber workforce members. As of August 2012, 220 high-school juniors and 168 seniors were enrolled in the program [Kay 2012].

These state-wide cyber workforce development programs are modeled to grow the industry and public awareness in their regions. These states will be able to attract more businesses and cyber professionals, and improve their local economy. However, while the programs and growth exist local to their region, the resulting effects—a better trained and prepared cyber workforce—will have a national impact.

4 Next Steps

It has been firmly established that the nation's cyber workforce is lacking in numbers and in talented individuals needed to effectively operate in cyberspace. There is also undeniable evidence that the U.S. is trailing behind other countries in preparedness and sophistication in the cyber domain. While several directives, frameworks, programs, and initiatives exist that are designed to grow, train, and retain a skilled cybersecurity workforce, there are some gap areas where further focus could contribute to attaining measurable success.

One gap area is the lack of specific job-role task details. Many of the training frameworks list specific job roles or functions that are similar across frameworks and favor the government sector. What is missing from most the job-function information are details on the specific tasks performed as part of that job role. What particular duties would one regularly perform while in that job role, and further, what skill level is required to be effective at those duties?

Once specific tasks are defined—including proficiency levels—training objectives and career training plans can be better devised. By knowing the skills necessary to operate competently within a functional role, individuals as well as organizations would be able to target training and skill exercises more effectively. The JCT&CS addresses this within mission-specific tasks that have proficiency-rated KSAs assigned, but this information has not matured to be publically accessible or industry applicable.

Another area that would benefit from further work is customized skill and performance assessments that are tailored for each job role and the associated tasks. Currently, evaluations exist to assess individuals' comprehension of knowledge-building material and even models that can measure accomplishment within skill and experience exercises. The assessment piece that is lacking is one that directly represents a job role and the associated tasks an operator would be expected to perform in cyberspace.

These assessments could be conducted before and after training activities. Pre-training assessments can help determine a baseline to compare post-training assessments against and serve as a tool for measuring the feasibility of the individual successfully accomplishing the requirements to be considered qualified to perform specific tasks. The pre-assessment could include knowledge and skill testing to gauge the individual's current comprehension of concepts and technologies, and also cognitive, Myers-Briggs-type testing. Certain tasks may be better performed by individuals with certain behavior or personality types; cognitive testing could help identify individuals who are a good fit.

While training and assessing individuals is crucial, cyber environments are maintained by a single individual. Most tasks function in conjunction with, or in support of, other job roles and tasks. Job roles are typically dependent on each other with overlapping duties. For this reason, team-based training and assessments are valuable because they provide more environment-realistic experience. Teams with individuals performing related or overlapping tasks would benefit from training together because it would provide exposure to the types of tasks that affect their duties and vice

versa. The CERT Division's STEPfwd helps with team training using simulated-environment, team-based exercises, but initiatives would do well to have related information that maps job roles to one another.

An additional oversight is the lack of representation of industry-specific job roles within the frameworks and directives. Development of a robust cyber workforce is an effort at the national level. In order for these frameworks to be relevant and applicable to industry or even academia, roles familiar to their sectors need to be included.

The work required to fill these gap areas includes identifying all the individual tasks performed within each job role and the skills and expertise needed to successfully perform these tasks. Once this information is captured, measures of success would need to be blueprinted to build assessments and training objectives against. It will be no small feat developing a matrix of assessment indicators for job-role tasks, but in order to make training more meaningful and have confidence in an individual's cyber operations capabilities, the efforts must be invested.

5 Conclusion

Every sector of the nation operating in cyberspace is acutely aware of the threats in this domain and the lack of enough people resources, or "human capital," who are adequately prepared to defend and protect critical systems and services. Threats in the form of incidental human or equipment error, or attacks launched with an end goal of service disruption, financial gain, espionage, or annoyance, are evolving in number and sophistication. The cyber workforce must mature in turn.

As previously reviewed, several workforce development directives and frameworks have been created to support cyber workforce training and development. All government and military personnel performing cyber duties, as well as a portion of industry and academia cyber professionals, are adhering to one or more of these directives either by mandate or as a best practice.

A small survey of training programs and other initiatives that support these directives or otherwise aid in cyber workforce growth and retention was introduced earlier. The options for obtaining knowledge and skills, and for experience building are advancing and customizable to the individual's or organization's need. Online courses available 24/7 from anywhere in the world and accessible via mobile devices, hands-on exercises to practice concepts, and virtual real-world simulated environments where users can practice engaging in operational scenarios are a few examples of the types of training available to the cyber workforce.

While many of these supporting initiatives are successful in terms of the number of people reached and the quality of cutting-edge materials and technologies available, they could be used more effectively if a direct relationship existed between the training programs and frameworks. Individuals are engaging in training on a regular basis but to what end? Currently, implementing training and skill- or experience-building exercises is a good practice, but it does not "stamp" an individual as qualified for a specific role: Hence, it will not reach General Alexander's goal of a workforce that is "trained to a standard and can accomplish the mission that is expected of them."

References

URLs are valid as of the publication date of this document.

[CyberCityUSA.org 2013]
CyberCityUSA.org. *CyberCityUSA San Antonio, Texas homepage*. http://cybercityusa.org/home (2013).

[DoD 2012]
U.S. Department of Defense. *DoD 8570.01-M, Information Assurance Workforce Improvement Program*. DoD, January 24, 2012.

[Hamill 2013]
Hamill, Jasper. "Verizon: 96 PER CENT of State-Backed Cyber-Spying Traced to China." *The Register*. http://www.theregister.co.uk/2013/04/23/spies_verizon_security/ (April 23, 2013).

[Hammerstein 2010]
Hammerstein, Josh & May, Christopher. *The CERT Approach to Cybersecurity Workforce Development* (CMU/SEI-2010-TR-045). Software Engineering Institute, Carnegie Mellon University, 2010. http://www.sei.cmu.edu/library/abstracts/reports/10tr045.cfm

[Homeland Security Advisory Council 2012]
Homeland Security Advisory Council. *CyberSkills Task Force Report, Fall 2012*. U.S. Department of Homeland Security, 2012. https://www.hsdl.org/?view&did=723343

[Kay 2012]
Kay, David J.; Pudas, Terry J.; & Young, Brett. "Preparing the Pipeline: The U.S. Cyber Workforce for the Future." *Defense Horizons 72* (August, 2012). http://www.ndu.edu/CTNSP/docUploaded/DH%2072%20for%20web.pdf

[Roman 2012]
Roman, Jeffrey. *Scholarship for Service Opportunities: SFS Program Director Offers Advice for Students*. http://www.careersinfosecurity.com/scholarship-for-service-opportunities-a-4616/op-1 (March 23, 2012).

[USCC 2010]
United States Cyber Command (USCC). *U.S. Cyber Command Concept of Operations*. http://itlaw.wikia.com/wiki/U.S._Cyber_Command_Concept_of_Operations (2010).