Commercial Cyber Certifications for Military Reserve Components

Dr. John A. Hamilton Jr., Mississippi State University

Dr. John A. Hamilton, Jr. is a Professor of Computer Science and Engineering and Director, Center for Cyber Innovation at Mississippi State University. Previously he was an Auburn Alumni Association Professor in Computer Science and Software Engineering at Auburn University with joint appointments in Management and Industrial and Systems Engineering. Dr. Hamilton was the founding director of the Auburn Cyber Research Center.

Mr. DeMarcus Montrez Thomas, Distributed Analytics and Security Institute

DeMarcus Thomas is a Research Engineer with the Distributed Analytics and Security Institute (DASI) at Mississippi State University. He holds a B.S. in Computer Science from Mississippi Valley State University and a M.S. in Computer Science from Norfolk State University. DeMarcus is currently pursuing a Ph.D in Computer Science from Mississippi State University. His research interests include: digital forensics, memory forensics, malware analysis, and applied machine learning.

Dr. Patrick Pape, Distributed Analytics and Security Institute

Assistant Research Professor with the Distributed Analytics and Security Institute (DASI) at Mississippi State University. He holds a B.S. in Computer Engineering from the University of Alabama in Huntsville, an M.S. in Computer Science with a minor in Information Assurance and a Ph.D. in Computer Science at Auburn University. His research interests include: machine learning, digital forensics, cybersecurity education, malware detection and analysis, and secure software development.

Commercial Cyber Certifications for Military Reserve Components: A Public-Private Partnership

By Drew Hamilton, Patrick Pape and Demarcus Thomas
Mississippi State University

Keywords

CISSP, CEH, CCNA Security, Security+, IASP, Cyber Certifications, Outreach, Workforce Development, Cyber Security,

Abstract

US Reserve Components provide the only viable cyber surge capability in the event of a nation-state level cyber attack. Reservists working in cyber are required to meet the training and certification requirements of DoD's Information Assurance Workforce Improvement Program. Mississippi State University is working with reserve component organizations across the country to assist their personnel in obtaining required civilian cyber security certifications. This paper will describe Mississippi State University's engagement with the US Army Reserve's Public Private Partnership Initiative (P3I) operated by the National Security Agency.

Background

The National Security Agency (NSA) also operates the National Center of Academic Excellence (NSACAE) in partnership with the Department of Homeland Security. Under the auspices of the National IA Education & Training Program, more than 130 colleges and universities are designated as National Centers of Academic Excellence in Cyber Defense Education, Cyber Defense Two-Year Education, Cyber Defense Research and Cyber Operations. Mississippi State University (MSU) is designated as a NSACAE in Cyber Defense, Cyber Defense Research and Cyber Operations. MSU is currently mentoring Mississippi Valley State University (an HBCU) through the multi-year NSACAE Cyber Defense Process and East Mississippi Community College through the NSACAE in Cyber Defense Two-Year Education.

Approximately fifteen of the more than 130 NSACAEs were invited to participate in a pilot Public-Private Partnership initially sponsored by the US Army Reserve and administered by the NSA. The US Reserve Components are comprised of the Army and Air National Guard and the US Army, Marine Corps, Navy and Air Force Reserves. (Non-DoD uniformed components are nor currently part of this program.)

The problem this program is trying to solve (or at least alleviate) is that the Defense Department has a critical shortage of educated and trained cyber personnel. Today's post-9/11 Reserve Components (RC) operate much differently then they did during the Cold War. As Lieutenant Colonel Jody Ogle, WVANG commented to me: the National Guard has

evolved from a strategic reserve to a constantly deploying force. The National Guard employs cyber protection teams nationwide who are frequently activated and deployed on real world cyber missions. So how do we credential this highly diverse, very mobile population with educational backgrounds varying from GED to Ph.D.?

Introduction

Increasingly, the Federal Government relies on the National Institute of Standards and Technology (NIST) standards to define cyber security policy including cyber security education and training. Figure 1 illustrates the NIST-prescribed Cybersecurity Learning Continuum.

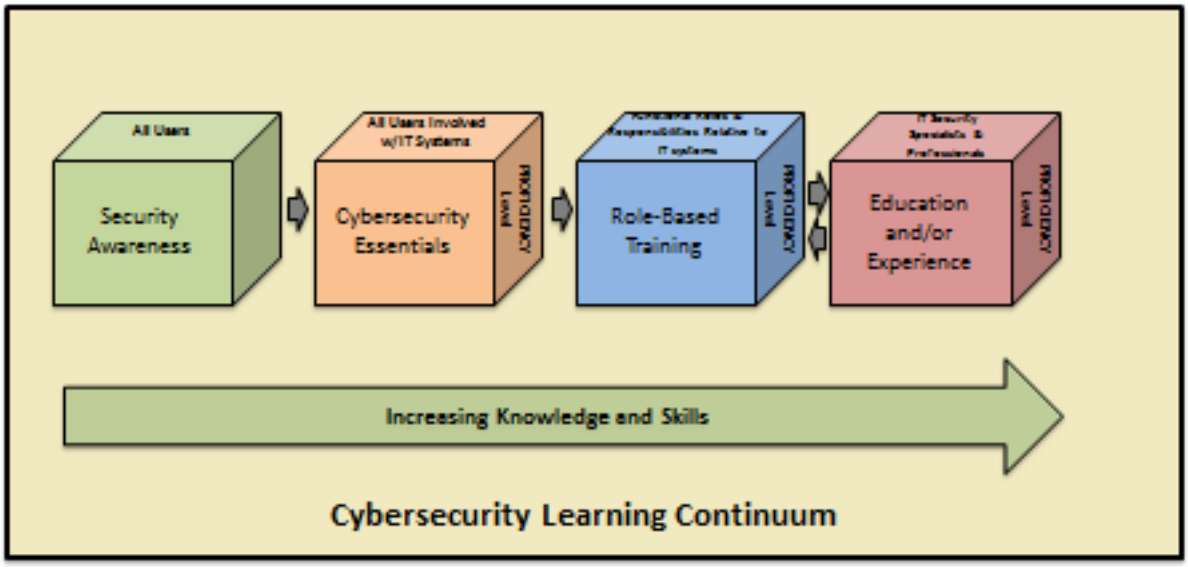

Figure 1. Cybersecurity Learning Continuum [1].

NIST defines the elements of the continuum above as follows:

- **Security Awareness** is explicitly required for all employees.
- **Cybersecurity Essentials** is needed for those employees, including contractor employees, who are involved in any way with IT systems. Cybersecurity Essentials is the transitional stage between "Basic Awareness" and "Role-Based Training."
- **Role-Based Training** becomes focused on providing the knowledge and skills specific to an individual's roles and responsibilities relative to Federal Organization information systems. Their role within the organization is primary with IT secondary. Decision responsibilities come from the organization role, whereas the technical responsibilities are derived from the relationship with IT.
- **Education** focuses on developing the ability and vision to perform complex multi-disciplinary activities and the skills needed to further the IT/cybersecurity profession and to keep pace with threats and

technology changes. This can be accomplished with experience, cooperative training such as "on the job" training or through certification and advanced education such as undergraduate and graduate studies and degrees as accepted by the particular Federal Organization. [1]

Security awareness is not specifically addressed in this effort. It is worth noting that virtually all military personnel and veterans have been exposed to security awareness training that is required to access any DoD computer system. NIST SP 800-50 further defines the Cybersecurity Learning Continuum in terms of their target audiences as shown in Figure 2 below.

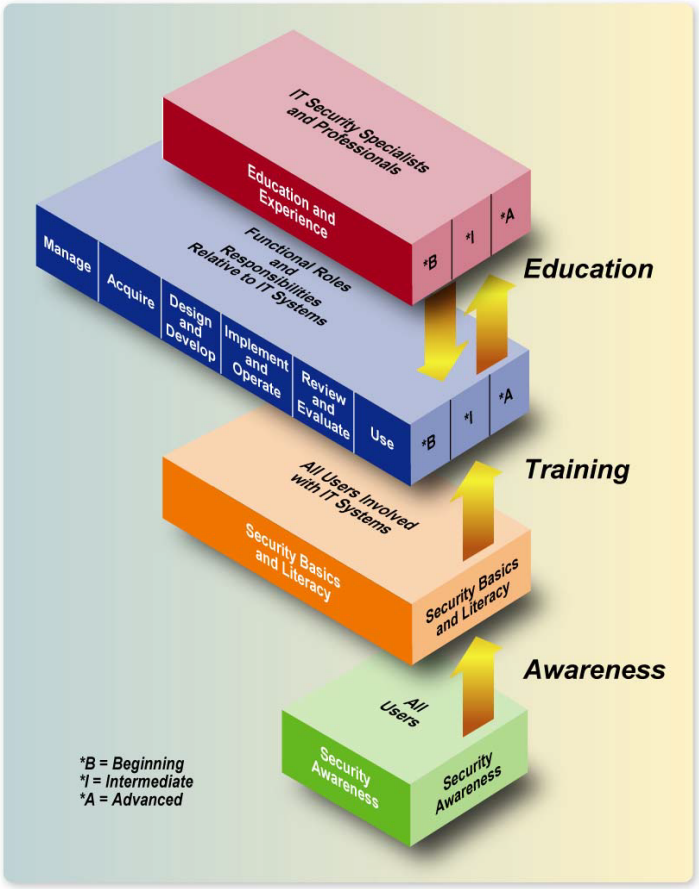

Figure 2. NIST 800-50 representation of the Cybersecurity Learning Continuum [2].

Figure 2 maps out the target audiences for each stage in the continuum as follows:

Security Awareness → All users
Security Basics and Literacy (now Cybersecurity Essentials) → All IT workers
Role-based → Specific skills based on individual roles and responsibilities
Education → IT specialists and professionals.

NIST 800-50 also outlines beginning, intermediate and advanced levels for role-based and education levels. The Department of Defense categorizes its cybersecurity workforce under Department of Defense Directive 8140.01 "Cyberspace Workforce Management [3]. DoDD 8140.01 cancelled DoD Directive 8570.01 "Information Assurance (IA) Training, Certification, and Workforce Management," [3]. But the corresponding 8570 instruction manual, DoDI 8570.01-M (incorporating change 4) remains current though heavily redlined [4]. This is a lot to sort through and the regulations and instructions are constantly changing. Of particular note are the DoD 8570 Baseline certifications shown in Figure 4 below [5]. However, DoD does prescribe baseline certifications to meet DoD 8570.01M certifications requirements that roughly line up against the NIST Cybersecurity Learning Continuum. As noted in Figure 3 below, current DoD guidance divides their workforce into Information Assurance Technical (IAT) and Information Assurance Management (IAM) tracks.

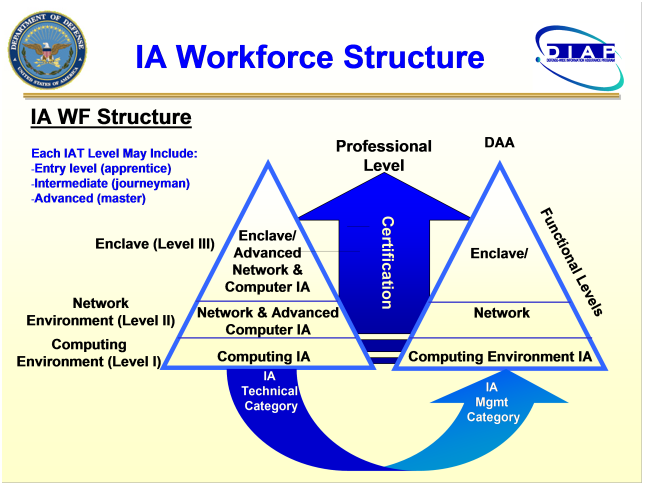

Figure 3. Overview of Basic IA Workforce Structure [4].

Meeting the Need Through Commercial Certifications

MSU's Cyber Certification strategy is roughly based on the training strategy used by the US Army. We are focused on four certifications: CompTIA's Security+ under development in partnership with the USAF 333rd Training Squadron at Keesler AFB; Cisco's Certified Network Associate – Security (CCNA – Sec) is under development with sponsorship of the National Security Agency, and our already fielded EC-Council's Certified Ethical Hacker (CEH) and ISC(2) Certified Information System Security Professional (CISSP). We will address each of these efforts in turn. On all of the MSU certification programs, we are working hard to produce study guides that do not use copyrighted material. This will help to overcome the high costs associated with commercially offered training and study guides and broaden the training opportunity for military and veterans. Although the exact policies vary by service, generally DoD will pay for the exam costs for Regular and Reserve personnel who have a DoD 8570-01M requirement for the certification.

CompTIA's Security+: Keesler AFB is Mississippi's largest military installation, and conducts cyber training for the Air Force and other DoD components. Elements of the 81st

Training Wing conduct " Security+ certification to cyberspace support Airmen prior to air expeditionary force deployments" [6]. At a minimum, MSU is committed to sharing Security+ training materials with the 81st Wing's 333rd Training Squadron. MSU's Security+ Program is designed to support our partnership with Mississippi Valley State University's (MVSU) an HBCU in the Mississippi Delta. MSU is working with MVSU to create a Security+ boot camp to support students to obtain the certification. The review course under development closely follows the six domains of the Security+ exam:

1. Network Security
2. Compliance and Operational Security
3. Threats and Vulnerabilities
4. Application, Data and Host Security
5. Access Control and Identify Management
6. Cryptography

The CompTIA Security+ certification is focused on providing capabilities to do the following: identify risks, perform risk mitigation activities, provide infrastructure, application, information and operational security, apply security controls to maintain confidentiality, integrity and availability, identify appropriate technologies and products, troubleshoot security events and incidents, and to operate with an awareness of applicable policies, laws and regulation [7].

Certified Ethical Hacker (CEH): For the past two years, MSU has been conducting 45 hour CEH Review Courses for the Mississippi and New Mexico National Guard with more than 100 participants. The CEHv9 certification is built around eighteen modules and is designed for personnel skilled at penetrating and finding vulnerabilities in systems [7].

1. Introduction to Ethical Hacking
2. Footprinting and Reconnaissance
3. Scanning Networks
4. Enumeration
5. System Hacking
6. Malware Threats
7. Evading IDS, Firewalls & Honeypots
8. Sniffing
9. Social Engineering
10. Denial of Service
11. Session Hijacking
12. Hacking Webservers
13. Hacking Web Applications
14. SQL Injection
15. Hacking Wireless Networks|
16. Hacking Mobile Platforms
17. Cloud Computing
18. Cryptography

Cisco Certified Network Associate – Security (CCNA-Sec): With support from the National Security Agency, MSU is developing a CCNA-SEC Review Course. This program is used by

the Army Cyber Center of Excellence at Fort Gordon to train their non-commissioned officers. The Cisco Certified Network Associate (CCNA) Security certification provides professionals with the skills necessary to create a security infrastructure, recognize threats on a network, and perform the actions necessary to mitigate those threats. The CCNA Security curriculum emphasizes core security technologies, the installation, troubleshooting and monitoring of network devices to maintain integrity, confidentiality and availability of data and devices, and competency in the technologies that Cisco uses in its security structure [8]. A CCNA Security certified employee is ready for roles such as Network Security Specialist, Network Security Administrator and Network Security Support Engineer. The certification exam is broken into six parts listed below [3].

1. Fundamentals of Network Security
2. Secure Access
3. Virtual Private Networks (VPN)
4. Secure Routing and Switching
5. Cisco Firewall Technologies and Intrusion Prevention System Technologies
6. Content and Endpoint Security

Certified Information System Security Professional (CISSP): A full discussion on all the DoD 8570-01M certifications is beyond the scope of this paper and likely beyond the scope of any single university. CISSP stands for Certified Information Systems Security Professional and the certification is administered by the nonprofit (ISC)2 organization. The US Army has incorporated CISSP certification in several of their courses at the US Army Cyber School at Fort Gordon, Georgia. Ten days of instruction in the Army's Cyber Basic Officer Leader Course is devoted to CISSP certification [9]. It should also be noted that CISSP contains material that was specified in the Committee on National Security Systems (www.cnss.gov) information assurance standards. The CISSP certification is built around eight domains [10].

1. Security and Risk Management
2. Asset Security
3. Security Engineering
4. Communication and Network Security|
5. Identity and Access Management
6. Security Assessment and Testing
7. Security Operations
8. Software Development Security

In evaluating the DoD-approved certifications shown in Figure 4 below, it is important to keep in mind the DoD differentiation between IAT and IAM. Also note the red strikeouts and red additions showing the dynamic nature of the DoD guidance. We are developing the Security+ Certification as an entry-level cert and to help meet the needs of Mississippi. We are specifically looking at extending our Security+ certification efforts beyond our work in the Mississippi Delta to specifically support credentialing high school teachers. Our other certification efforts directly line up with the approved DoD 8570 baseline. It is clear that the CISSP certification shows in the most career boxes. For the Information Assurance workforce specified in the DoD 8570.01-Manual, CCNA Security is a baseline certification

for IAT Level I & II. CEH supports specific roles as outlined in NIST SP 800-16[1] as well as DoD 8570.01M

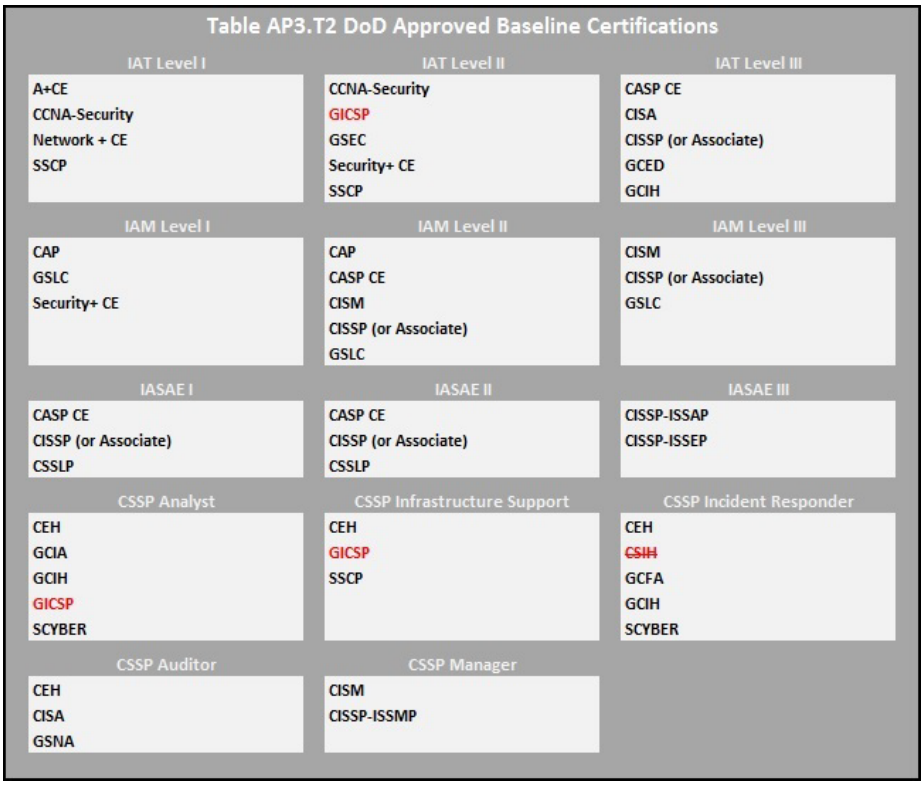

Figure 4. DoD Approved 8570 Baseline Certifications [4] [5].

Meeting the Need for Cybersecurity Education

Recall that in Figure 1 we illustrated the NIST CyberSecurity Learning Continuum. Education was at the top of the continuum and included degrees as well as certifications. As part of the NSA's Cyber P3I partnership, MSU is offering Reserve Component personnel full scholarships to enroll in MSU cyber security degree programs. This program is open to all members of the Reserve Components except for members of the Individual Ready Reserve and the Retired Reserve.

Reservists and Guardsmen (hereinafter referred to as Scholars) selected for the program will receive one-year scholarships, with an option to continue contingent upon receipt of additional program funds:
1. Tuition
2. Mandatory or general fees as determined by the institution. Optional or miscellaneous fees will not be covered.
3. Book allowance
4. Travel funding for one cybersecurity conference per academic year to continental US-held conferences only.

5. One-time cost of laptop or tablet for coursework and/or electronic books (returning scholars who continue from prior year(s) and/or continue for an additional degree/certificate will only receive one laptop)

Right now this program is focused on our distance education – offered Master of Science in Information Systems program, but we are working to expand our distance-ed certification and degree options. Currently we are getting applications from reservists and guardsmen from Kabul, Kosovo as well as closer to home like Kosciusko, Mississippi.

Conclusions

The MSU effort is an outstanding example of a public private partnership. Through this effort, MSU has been able to assist reservists/guardsmen achieve mandated commercially recognized cyber certifications. Cyber certifications can provide an important incentive/reward for reserve personnel and improve retention.

MSU has successfully offered 45 hour Certified Ethical Hacker (CEH) and Certified Information System Security Professional (CISSP) review courses to National Guard members. In partnership with the NSA CAE Program, the MSU Center for Cyber Innovation and the MSU College of Business, MSU is offering Reserve Component Personnel the opportunity to complete for NSA-sponsored cyber scholarships. MSU is covering many of the IAM (Management) and IAT (Technical) DoD workforce requirements as well as full spectrum of the NIST Cybersecurity Learning Spectrum.

DoD requires cyberspace workers to meet certification requirements. This requirement applies to uniformed military personnel, DoD civilians and contract cybersecurity service providers (CSSPs). Demand for certification training is currently overwhelming internal DoD training capacity [11]. Through the NSA's P3I program, MSU is contributing to the workforce development necessary to meet the need for a trained and educated cyber workforce.

Acknowledgments

This work made possible by the generous support of the National Information Assurance Education and Training Program under Contract NSA # H98230-17-1-0375.

References

[1] *NIST Special Publication 800-16 Revision 1 (3rd Draft),* Toth, Patricia and Klein, Penny, "A Role-Based Model for Federal Information Technology/ Cybersecurity Training," US Department of Commerce, March 2014.

[2] *NIST Special Publication 800-50,* Wilson, Mark and Hash,Joan, "Building an Information Technology Security Awareness and Training Program," US Department of Commerce, October 2003.

[3] *DoD Directive 8140.01 Cyberspace Workforce Management*, DoD CIO, Washington, D.C. August 11, 2015.

[4] *DoD 8570.01-M Information Assurance Workforce Improvement Program*, ASD(NII)/DoD CIO, December 19, 2005, incorporating change 4 dated November 10, 2015.

[5] *DoD Approved 8570 Baseline Certifications,* Defense Information System Agency's Information Assurance Support Environment published at: https://iase.disa.mil/iawip/Pages/iabaseline.aspx accessed February 4, 2018.

[6] "New Security+ certification course offered at Keesler AFB," 81st Training Group Public Affairs, http://www.af.mil/News/Article-Display/Article/113832/new-security-certification-course-offered-at-keesler-afb/ accessed February 4, 2018.

[7] "CompTIA Security+ Certification Exam Objectives." [Online]. Available: https://certification.comptia.org/docs/default-source/exam-objectives/comptia-security-sy0-401.pdf accessed: February 2, 2018.

[8] Walker, Matt, All-in-One CEH Certified Ethical Hacker, 3rd Edition, McGraw-Hill, New York, 2017.

[9] Levering, Laura, "Army Cyber School Marks Major Milestone," US Army Web Page https://www.army.mil/article/154001/Army_Cyber_School_marks_major_milestone accessed 22 March 2017.

[10] Gordon, Adam, *Official (ISC)2 Guide to the CISSP CB*K, CRC Press, Boca Raton, Fla. 2015.

[11] Hamilton, John A., Jr. and Pape, Patrick R. , "Reserve Component Cyber Certification," *2018 ASEE Southeastern Section Conference*, Daytona Beach, Fla., March 4 – 6 2018.