Reserve Component Cyber Certification

J.A. "Drew" Hamilton, Jr., Ph.D. and Patrick R. Pape, Ph.D.
Mississippi State University

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 in Mississippi and New Mexico 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).

Keywords

CISSP, CEH, IASP, Cyber Certifications, Outreach, Workforce

INTRODUCTION

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.

Mississippi State University (MSU) has a long history of engagement with the Department of Defense. Through the National Science Foundation's CyberCorps program, MSU's implementation of a Cyber Master of Science program for Regular Navy officers and the National Security Agency's Information Assurance Program, MSU has placed a large number of its graduates in DoD cyber positions or in companies that support DoD Cyber Operations. MSU is one of sixteen schools nationally certified by the NSA as Center of Academic Excellence in Cyber Operations.

BACKGROUND

Department of Defense Directive 8140.01 "Cyberspace Workforce Management" prescribes roles and responsibilities for cyberspace workforce management [1]. DoDD 8140.01 cancelled DoD Directive 8570.01 "Information Assurance (IA) Training, Certification, and Workforce Management," [2]. But the corresponding 8570 instruction manual, DoDI 8570.01-M (incorporating change 4) remains current though heavily redlined [3]. There is another layer of indirection as DoDI 8570.01-M points the reader to a Defense Information Systems Agency (DISA) web site for the current list of approved certifications. The web site is hosted under DISA's Information Assurance Support Environment under DoD Approved 8570 Baseline Certifications at http://iase.disa.mil/iawip/Pages/iabaseline.aspx [4].

Critical to understanding the certification requirement is understanding the way DoD categorizes its cyber workforce. While DODI 8570-01 is scheduled for updating, it is still in effect and defines the workforce in the categories listed in the Baseline Certifications chart. Government employees are classified first as either information assurance technical (IAT) or information assurance management (IAM). Figure 1, based on DoDI 8570.01-M shows the three IAT and IAM levels that are explicitly defined in the manual [5]. The IASE FAQ website provides important clarification of the Information Assurance System Architect and Engineers (IASAEs) specialty that also has three levels and is defined in DoDI 8570.01-M. As noted in [5]: "The CSSP specialty levels are tied to functional positions, i.e., Analyst, Infrastructure Support, Incident Responder, Auditor, and Manager.

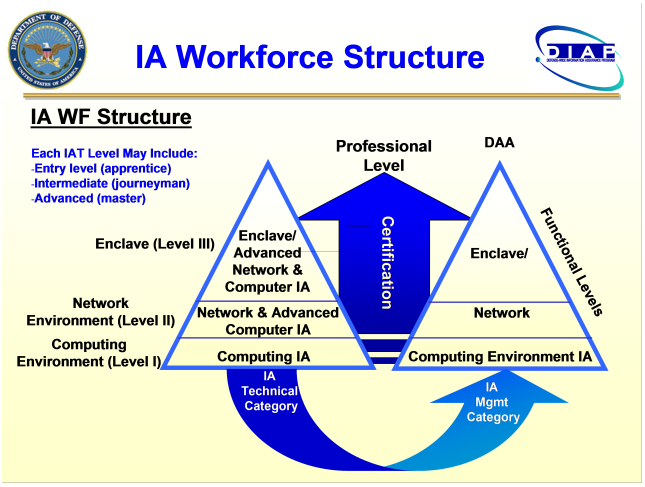

Figure 1. Overview of Basic IA Workforce Structure [3][5].

The DoD prescribed baseline certifications are shown in Figure 2. A full discussion on all the listed certifications is beyond the scope of this paper. However, it is clear that the CISSP certification shows in the most career boxes. 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 [6]. 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 [7].

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

The Certified Ethical Hacker (CEH) certification also appears in many of the career boxes in Figure 2.

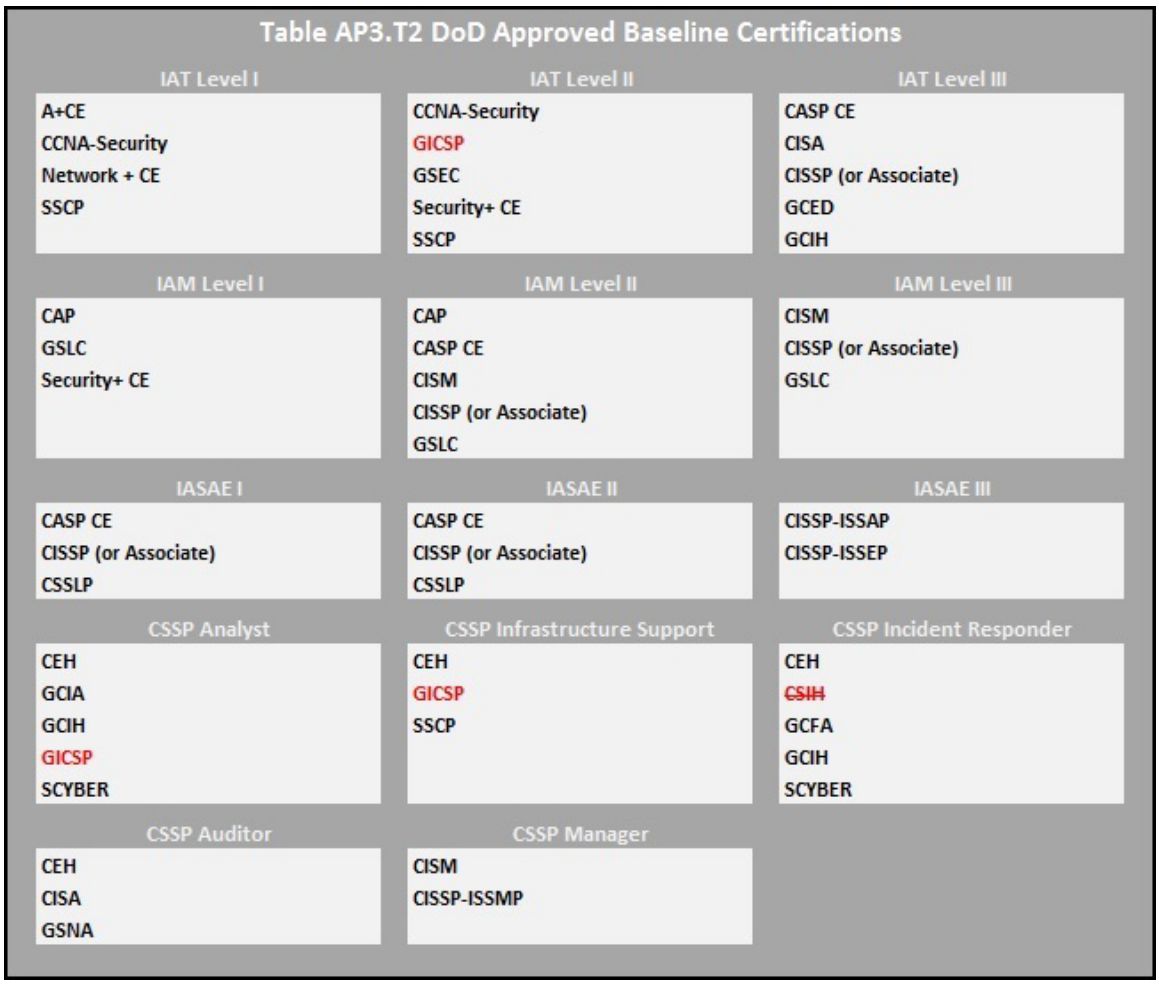

Figure 2. DoD Approved 8570 Baseline Certifications [4].

CEH is administered by the EC-Council. CEH certification also appears in many Army courses at the Cyber Center of Excellence at Fort Gordon. The Army's Credentialing Opportunities On-Line (Army Cool) Program list six enlisted and three warrant officer military occupational specialties (MOS) that contribute to attaining the CEH certification. The CEHv9 certification is built around eighteen modules [8].

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

Against this backdrop, the US Army Reserve's Public Private Partnership Initiative (P3i) engaged the NSA's National Information Assurance Education and Training Program (NIETP) to reach out to cyber schools which was done at the 2016 National Cyber Summit in Huntsville. The P3i - NIETP effort, initiated several university projects.

Under previous NIETP and NSF supports, MSU has developed strong expertise in deeply technical outreach as well as cyber awareness and familiarization with less technical military and wounded veteran participants. Mississippi State University teamed with the University of New Mexico as part of a continuing MSU-UNM effort. In a previous effort, UNM faculty from the Anderson School of Management, Steve Burd and Alex Seazzu supported MSU efforts to establish a digital forensics program at Western New Mexico University.

Figure 3. MSU's Patrick Pape conducting NSF funded digital forensics workshop at UNM [10].

The National Science Foundation project involved building demand for the digital forensics program by conducting workshops for New Mexico. Many of the participants in these workshops were members of the New Mexico National Guard. This current MSU-UNM effort was inspired by these interactions.

DoDD 8140.01 directs DoD components to track and report the qualifications of "for military, DoD civilian, and contractor support personnel who perform cyberspace work roles [1]." Mandating commercial certifications is one thing, meeting that mandate is another.

DoD and the Army in particular already conduct outstanding cyber training to include courses at Fort Gordon, Ga. and Camp Robinson, Ark. However this training is not always accessible by reservists and guardsmen.

Senior leaders from both the Mississippi National Guard and New Mexico National Guard report that the available training courses are over-subscribed and have waiting lists. Major General Bosse, Commanding General of the Army Reserve's 335th Signal Command, commented that travel costs were also an issue and training closer to home stations was desirable [11]. MG Bosse commands all cyber units assigned to the US Army Reserve.

Figure 4. Army Cyber "Triad."

Figure 4 provides a very simplistic explanation of the three major cyber efforts in the Army. The Army Cyber Institute based at the US Military Academy, West Point, has already established itself as a thought leader in the field of cyber operations. Civilian universities have access to a different talent pool than ACI and can complement the innovative ideas and concepts. While civilian universities do not engage in cyber operations as does Army Cyber Command and 2nd Army, this project has us closely working with some of the reserve component personnel who would work with ARCYBER in the event of a national emergency. Finally, the training materials developed under this project may be useful to the institutional "schoolhouse" at Fort Gordon's Cyber Center of Excellence.

PROGRAM EXECUTION

In our current effort, MSU will conduct a CISSP Review Course and a CEH Review Course for reserve component personnel in Mississippi and in partnership with UNM will conduct the same two courses for reserve component personnel in New Mexico. Our initial engagement has been with the National Guard leadership in each state. The initial courses will have been delivered before the 2018 ASEE-SE Conference and the results presented at the conference.

While training opportunities for the commercial cyber certifications are limited, DoD funding for testing is not. Therefore this project does not address the mechanics of certification testing.

Most importantly, this project supports the DoD Information Assurance Scholarship Program (IASP) [12]. When funding is available, IASP provides scholarships for cyber-related degrees for personnel willing to serve a government service obligation. For reservists/guardsmen, the service obligation is two years of service in the reserves for each year of scholarship. For those participants in the active guard and reserve program (AGR) the service obligation is one year of service for each year of scholarship.

Diversity is always an important consideration in any university project. DoD in general is a model of diversity. For this particular project it should be noted that Diversity is straightforward in states such as Mississippi and New Mexico. Mississippi has proportionately the highest African-American population (>37%) in the United States. New Mexico has the highest minority population in the US (48% Hispanic, 10% Native American).

CONCLUSIONS

This effort is an outstanding example of a public private partnership. Through this effort, two state universities are able to assist reservists/guardsmen in their states achieve mandated commercially recognized cyber certifications. Cyber certifications can provide an important incentive/reward for reserve personnel.

This project will build a pool of diverse IASP applicants currently serving in the Reserve Components. We will build this pool by offering the previously described cyber courses to reserve component personnel in Mississippi and New Mexico in partnership with the University of New Mexico, a Hispanic Serving Institution (HSI). Working through the Mississippi National Guard and New Mexico National Guard we will offer cyber training courses to reserve component personnel statewide, These courses will not only contribute to the cyber readiness of the Guard and Reserve, it will also provide Mississippi State University (MSU), University of New Mexico (UNM) with an identified pool of candidates from the reserves to compete for IASP scholarships.

This project assists in meeting the national demand for a cadre of professionals with hard skill cyber credentials. The ability to earn and obtain highly marketable commercial cyber certification can be an important recruitment/retention tool for the reserve components. Perhaps most importantly, this project provides the opportunity to give back to our servicemen and women who have given so much already to their country.

ACKNOWLEDGMENTS

This work made possible by the generous support of the National Information Assurance Education and Training Program under Contract NSA # H98230-16-1-0355.

References

[1] *DoD Directive 8140.01 Cyberspace Workforce Management*, DoD CIO, Washington, D.C. August 11, 2015.
[2] *DoD Directive 8570.01 Information Assurance (IA) Training, Certification, and Workforce Management*, ASD(NII)/DoD CIO August 15, 2004, certified current as of April 23, 2007.
[3] *DoD 8570.01-M Information Assurance Workforce Improvement Program*, ASD(NII)/DoD CIO, December 19, 2005, incorporating change 4 dated November 10, 2015.

[4] *DoD Approved 8570 Baseline Certifications,* Defense Information System Agency's Information Assurance Support Environment published at: http://iase.disa.mil/iawip/Pages/iabaseline.aspx accessed 22 March 2017.
[5] *DoD Instruction 8570.01-M Manual Information Assurance Workforce Improvement Program and DoD Directive 8140.01 Cyberspace Workforce Management FAQs,* Defense Information System Agency's Information Assurance Support Environment published at: http://iase.disa.mil/iawip/Pages/iaetafaq.aspx accessed 22 March 2017.
[6] 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.
[7] Army Credentialing Opportunities On-Line (Army Cool) . https://www.cool.army.mil/search/CERT_CEH4310.htm Accessed 22 March 2017.
[8] Gordon, Adam, *Official (ISC)2 Guide to the CISSP CB*K, CRC Press, Boca Raton, Fla 2015.
[9] Walker, Matt, All-in-One CEH Certified Ethical Hacker, 3rd Edition, McGraw-Hill, New York, 2017.
[10] Lynch, David, "Cybersecurity workshop draws students of various stripes from across state, " *UNM Daily Lobo*, September 3, 2015, http://www.dailylobo.com/article/2015/09/cybersecurity-seminar-at-unm Accessed 22 March 2017.
[11] Bosse, Major General Peter A., comments made during P3I Principal's Meeting, Fort Belvoir, Va,, 16 March 2017.
[12] *DoD Instruction 8145.01 DoD Information Assurance Scholarship Program,* DoD CIO, Washington, D.C., January 17, 2012.

Dr. Drew Hamilton is the Director of the Center for Cyber Innovation at Mississippi State University and a professor of computer science and engineering. Previously he held faculty appointments at Auburn University and the US Military Academy and a visiting appointment at the US Naval Postgraduate School. Dr. Hamilton earned his doctorate in computer science from Texas A&M University. Dr. Hamilton is a distinguished graduate of the Naval War College.

Dr. Patrick Pape is an 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.