TRAINING AND EDUCATING THE DoD CYBERSECURITY WORKFORCE

Ryan R. Wagner and Stephen M. Olechnowicz

The Problem

As technical training and associated certifications continually and rapidly evolve, DoD is challenged to ensure its workforce is appropriately and robustly credentialled in ways most suitable to providing secure networks.

Just as well trained and educated people are often the key to success in conventional conflicts, the same holds true for cyber warfare. DoD's information assurance (IA) and cybersecurity workforce are charged with defending DoD's cyber infrastructure and data from threats posed by a range of adversaries.

The cybersecurity positions, categories, and specialties... must evolve with the environment. Certifications that lose relevance... will need to be removed... and the bar for entry to new certifications should be raised...

Who Makes Up the IA Workforce?

IDA's involvement with IA and cybersecurity workforce issues stretches back to 1998, when it led the first comprehensive study on DoD IA personnel. Since then, IDA has helped DoD expand, train, and professionalize the IA workforce.

One of the perennial debates regarding the cyber workforce is the definition of whom it includes. A narrow view would focus on only those who spend most of their time on IA issues, such as information system security architects, intrusion detection system log analysts, and incident handlers. A broader view of the workforce includes any individual with privileged (administrative) access to an information system. In 2004, DoD Directive 8570, "Information Assurance Training, Certification, and Workforce Management," took the broader approach and mandated that "Privileged users and IA managers shall be fully qualified…, trained, and certified to DoD baseline requirements." This definition of the workforce covers military personnel, civilians, and contractors – more than 100,000 people, some deployed in theater and others working in the major network operations and security centers in the United States. The policy further directed the creation of a companion Manual[1] that defines a series of categories, specialties, and job functions for the IA workforce. The decision was made to use industry cybersecurity certifications rather than have DoD create its own.

One of the major challenges in the creation of the Manual was to identify and verify the industry certifications that meet the Manual's requirements. During the development of the Manual, IDA developed a robust methodology for systematically assessing the certifications for their applicability to workforce

[1] DoD 8570.01-M, *Information Assurance Workforce Improvement Program.*

categories, levels, and specialties. The methodology includes analyses of certification course material, labs, proprietary exams, and interviews with practicing professionals holding the certifications. IDA continues to be DoD's trusted resource for independent analyses of a wide variety of both managerial and technical certification offerings.

In concert with the American National Standards Institute (ANSI), IDA helped develop International Organization for Standardization/ International Electro-technical Commission (ISO/IEC) 17024, "Conformity assessment – General requirements for bodies operating certification of persons," which set out a series of requirements that ensure certification vendor quality, and that the certifying body is independent of the training provider. The standard was designed with cybersecurity certifications in mind, and the DoD now requires that certification vendors are accredited in compliance with the ISO 17024 standard.

As a result of interactions with IDA researchers, major IA certification vendors have enhanced their course material and exam questions. The goal is to ensure that successful completion of a certification requires a person to draw from various cybersecurity disciplines to apply their knowledge and demonstrate analytical skills. This helps ensure that certification holders have not simply engaged in rote memorization but rather have an operational understanding of cybersecurity.

As information technology and information assurance race ahead, IDA has been actively involved in updates to the Manual. This year, IDA researchers were part of a team involved in redefining the specialty profession of Information Assurance System Architect and Engineer (IASAE). The resulting draft certification constitutes a major change to the specialty in an effort to reflect changes to and new understandings of the IASAE roles. The draft recommends a mix of training and formal education for prospective IASAEs.

The Future of the DoD Cybersecurity Workforce

The relentless pace of progress in IT is bringing numerous new capabilities to DoD's doorstep, each with a variety of additional security concerns. The movement of IT from a custom, in-house service to a commercial commodity is also changing the field. The cybersecurity positions, categories, and specialties, along with their associated functions, must evolve with the environment. Certifications that lose relevance or fail to stay current will need to be removed from the Manual, and the bar for entry to new certifications should be raised as the field of commercial cybersecurity certifications grows more competitive.

From having performed one of the first studies on the workforce over a decade ago to today's research on the future of the field, IDA is working closely with DoD to ensure that it has a plentiful pool of highly-trained IA experts to defend its networks and ensure the success of its missions.

Mr. Wagner and Mr. Olechnowicz are research staff members in IDA's Information Technology and Systems Division. Mr. Wagner holds a master of engineering degree from the Massachusetts Institute of Technology and has worked as a senior security engineer with Verizon Business.