DoD Offers Useful Certification Guidelines

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

MSIA graduate (class of 2007) Jacqueline R. Tregre is a Senior Information Assurance Engineer with the US Army in Arizona. She has very kindly contributed the following article to the column. The remainder of today’s posting is entirely her work (with minor edits).

* * *

One of the difficult questions facing employers today is, "How much training is enough?" The Department of Defense (DoD) put its considerable resources into that very question and produced the "Information Assurance Workforce Improvement Program" manual, DoD 8570.01-M.[1] This manual, publicly available, calls out for industry standard certifications (and implicitly for the training to attain them) for both the technical personnel that actually put hands on systems, and for the management personnel responsible for running the organization’s information assurance (IA) Program.

This development is important to private industry because if these levels of certification are required for the operation of the government, then it is reasonable to believe these levels will eventually become a de facto standard for industry. The DoD 8570 defines categories and specialties within the IA workforce, and certifications in both the computing and/or network environments and in the information assurance arena. For example, if someone is an enterprise administrator (Domain / Forest Administrator), s/he should be certified in the operating system (OS) that s/he administers, plus any applications administered in that computing environment. Furthermore, due to the extensive responsibilities of the individual, DoD 8570 demands that administrators (technically IAT-III, standing for IA Technical Level III) obtain suitable certifications; options include CISSP,[2] CISA,[3] SCNA,[4] or GSE[5].

The IA Manager category, or IAM, is responsible for IA policy, procedures, and the information technology (IT) workforce structure and training. The IAM-III requires the GSLC,[6] the CISM,[7] or the CISSP. Certifications such as these demonstrate that your IAM has the broadly scoped knowledge necessary to make prudent and reasonable decisions in information and network security policies and procedures.

The DoD 8570 certification requirements for Level III are the highest-level requirements; it also recognizes levels II and I. These roughly correlate to Enterprise Level (III), Network Level (II), and System Level (I). The DoD 8570 elaborates further on position requirements such as Experience, Knowledge, Supervision, and Other such as independence in actions. For example, the IAT-I works entirely within established policies and procedures, while the IAT-II "relies on experience and judgment to plan and accomplish goals within the [Network Environment]."[1] [pg 27]

The manual helpfully lists functions executed by each category and level. A supervisor may use these in writing job descriptions or especially in defining personnel ratings and rating standards. For example, the DoD 8570 lists 31 functions for the IAT-II position. One may establish standards with each function, such as, "T-II.20. Perform system audits to assess security related factors within the NE."[1] [pg 28], and add the words "every x days or less" to establish a standard.

Your Chief Information Security Officers (CISO) may also take these requirements to argue successfully for resources from the Chief Operating Officer (COO) or Chief Financial Officer
The DoD 8570 gives management a good picture of what training the firm may deem as necessary, good to know, or non-essential.

If your organization receives, processes, stores, displays, or transmits DoD information, then the DoD 8500-series requirements apply to you, including these training requirements. If these requirements do apply, then consider having at least one person in your IT shop attain the Information Systems Security Engineering Professional (ISSEP) concentration certification of the CISSP. The ISSEP certifies an individual in knowledge of the NIST and DoD information assurance requirements. This level of knowledge could help your firm avoid a costly misstep in handling DoD information.

REFERENCES


[2] International Information Systems Security Certification Consortium (ISC)². (ISC)² is the official organization that maintains and administers the CISSP certification exam. See https://www.isc2.org/cgi-bin/content.cgi?category=97


[4] Sun Certified Network Administrator; see http://www.sun.com/training/certification/solaris/scna.xml


* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www2.norwich.edu/mkabay/index.htm >.

Army Major (Retired) Jacqueline Tregre, MSIA, BSEE, ISSEP, was a Signal Corps Officer until 2004, and now continues ‘the fight’ as a Department of the Army Civil Service Computer Engineer in the Information Assurance arena.

Copyright © 2008 Jacqueline R. Tregre & M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.