Proceedings of the 9th Colloquium for Information Systems Security Education
Georgia Institute of Technology
Atlanta, Georgia, 6-9, June 2005

A Strategy for Meeting DoD 8570.1-M Requirements

Leigh Armistead, *Honeywell* and Dennis Stone, *Thomson NETg*

Abstract – On 15 August 2004, DoD Directive 8570.1 Information Assurance Training, Certification, and Workforce Management was issued which required the training and education the IA Workforce with the appropriate tracking and certification mechanisms. This is a massive task and to date no clear guidance has been released directing how the military services should accomplish this task. This *document explains a methodology to approach* this requirement that maps existing military courses with CNSS IA Standards and offers a process to allow seamless use of existing classes with web-based courses to fulfill the directive.

Index terms – IA Standards, DoD 8570.1-M, IA Training

I. Introduction

The Department of Defense (DoD) Directive 8570.1 *Information Assurance Training, Certification, and Workforce Management* was released last year and will revolutionize the management and certification of Information Assurance (IA) professionals across the military services over the next five years [1]. This instruction mandates the training and mapping of the IA Workforce across the DoD and is designed to increase the quality and level of computer security education knowledge of these personnel. It is an attempt by the Office of Secretary of Defense (OSD) to ensure that the military understands and retains the right people to conduct operations in the Information Age. If done correctly, this directive can revolutionize the manner in which the DoD trains and manages its workforce in the future.

II. Background

It is readily apparent to the casual observer that IA is critical to the protection of the DoD networks and data resources. Current training programs are providing only a small fraction of the overall number of professionals needed. This shortfall is only getting worse as noted in the 8570 directive, thus lending the military services and the nation to an ever increasing state of vulnerability. Failure to close this gap affects information security across the enterprise, leaving the DoD and the national security apparatus vulnerable to mishaps and attacks.

This directive is an attempt to correct that deficiency. Once the follow-on manual is released by OSD, this second portion of the instruction will lay out how the services are supposed to meet the new requirements laid upon them. The DoD is currently reviewing the proposed 8570.1-M Information Assurance Training, Certification and Workforce Management Manual, and it should be released this summer. It will require all personnel – military, civilian and contractor – to be trained and certified within five years. Personnel will primarily be divided into two categories, technical and managerial, with three classes or levels per group. In addition, the new manual will provide guidance and procedures for the training, certification and workforce management of the DoD Information Assurance workforce, as well as information and guidance on reporting metrics and the implementation schedule for reference.

This Manual, that is in it's 26th revision, applies to the Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the Department of Defense Field Activities and all other organizational entities within the Department of Defense.

Thus in order to meet critical security needs for IA workforce as outlined in the DoD directive, the military needs to train thousands of Information System Security Managers and Officers, Designated Approval Authorities and System Administrators. Compounding this problem is the fact that there are only limited funds and limited instructors available, thus leading to the belief that these finite resources must be used in the most effective manner. Therefore many proponents of training within the military believe that the DoD needs a cost-effective and rapidly deployable strategy for closing this gap. It must be a process that can be accepted in the field, onboard ships at sea or while in garrison; all the while abiding by DoD mandated standards, and utilizing previously developed courses. In addition, the training and qualification of this IA workforce will depend on a clear understanding of the job requirements, the skills needed, industry standards for training and qualification, and the individuals' current skill level.

ISBN 1-933510-99-4/05/$15.00

Unfortunately this capability does not currently exist in the DoD. Today IA training is often characterized by tremendous amounts of confusion caused by a lack of standards and multiple certifications offered by several vendors. Organizations don't train for a myriad of reasons, such as not being certain which certifications match their needs, or that they want to avoid their staff being trained to meet certifications rather than meet the organizations needs. In most cases the process of analyzing the certifications is very time consuming and normally needs continually change. Many commands thus feel that training time and funds can be wasted on irrelevant certification training. Yet, they also feel that training targeted to the organizations needs will result in a better-trained staff at much less cost in both time and money. All of these reasons and more amount to a reluctance to spend valuable dollars on processes which could lead directly to recognizable results and are important at the deck-plate level, so any solution must address a procedure that directly meets DoD requirements. In this paper, a proposed comprehensive methodology is provided that targets training using a blended approach of instruction and media that is the most cost and time effective for the military services.

III. Effects of DoD 8570.1-M

Once released, this Manual will be effective immediately, and it will be mandatory for use by all DoD Components. In it's current draft form, as noted earlier, the manual describes two major career tracks; IA Technical (IAT) and IA Managerial (IAM). Each has three levels, and twenty to forty skills associated with each, such as this example - "Implement and monitor IA safeguards for CE system(s) in accordance with implementation plans and standard operating procedures." The tasks in both tracks contain both management and professional development skills.

- IA Technical I, II and III (IAT)
- IA Management I, II and III (IAM)

DoD 8570.1 will also require that the training and certifications be managed and tracked. To date the directive does not specify how each entity will accomplish the goals. The manual is supposed to answer this question. Typically the DoD directs initiatives and states performance requirements, but leaves it to the individual entities or military services to meet the requirements in their own manner. The commands and units sometimes cooperate but typically have their own solutions. This specific proposal addresses a solution that cannot only be utilized in an enterprise wide approach, but also down to the deck-plate level. It allows individual commands to use curriculum that they are familiar with and understand, yet still meet the overall requirements. This option also allows organizations to develop new material that can be included into the service's training capability.

The capabilities to tailor the training are very important and need to be addressed because, as noted elsewhere, this directive is designed to improve the security of the military infrastructure and DoD. It is supposed to simplify the training support while lowering costs. However, there are critical components for closing this current gap in training capabilities that must be accepted by all for any proposed solution. From the author's perspective, each of these needs is addressed using industry best practices and leading edge technologies to keep costs low, impact high, and ongoing maintenance and support minimal. To do this, the following critical components are listed below:

- Clear, valid definition of the job requirements, maintained on a regular basis. A formal job analysis will define this quickly and objectively.
- Objective assessment of the actual skills of the target workforce. Newer automated tools make this easier with features such as employee-self-service, and intelligent, adaptive assessments.
- Automated gap analysis. Objective baselines, compared to the actual job requirements will help define the scope of training resources that should become a part of the solution.
- Automated training prescription that targets the right off the shelf training, using blended-learning approaches, to close individual skill gaps and provide credentials to those qualified. Automated tools now can provide this information and actually link the user to the order or begin the courses.
- Automated tracking, credentialing, and reporting to facilitate programmatic oversight.
- Executive sponsorship and a strong communications strategy and plan are critical to building momentum for the program.

IV. Training Available Today

As it stands today, with the release of the 8570 directive, each military service will be required to meet these new requirements within the five year time period. There are obviously different ways to do this, and in fact most commands and organizations have already developed a wide variety of IA training classes and curriculums, typically tailored to their own best practices. For example, each service has developed some sort of Information Systems Security Manager (ISSM) course used to certify their personnel to manage their networks and programs. These courses were obviously developed prior to the release of DoD 8570.1 and most likely will

ISBN 1-933510-99-4/05/$15.00

meet some of the skill requirements for the two main career tracks. **However, and this is key to this approach, most of these courses do not meet the entire Committee on National Security Standards (CNSS) 4014 standard and therefore some sort of additional training will be needed to comply with the DoD directive.**

The problem is that each service must provide an answer to the question of how does the respective IA workforce obtain these IAT and IAM qualifications? As this audience understands, there are many ways that one can receive a CNSS certification. Traditional classroom courses such as at the National Defense University (NDU) or any one of the National Security Agency (NSA) approved universities qualify in this category. Other brick and mortar training can be obtained through commercial vendors such as SANS that are paid for through a variety of sources. Web-based or distance learning courses are available as well, with examples such as Karta, who offer a complete 4013 course online. All of these avenues offer different opportunities for individuals to meet the 8570.1 requirements; assuming that the DoD eventually determines that the CNSS standards are the de facto baseline.

V. Proposed Methodology

So whatever the method decided upon by OSD and services to meet the requirements of 8570.1, the goal of any proposal would be to incorporate courseware already developed and in place. To date, neither OSD nor the military services have decided definitively what certification, skill sets or standards will map to the IAT or IAM tracks. However both the Navy and Marine Corps are advocating the use of the National Security Agency 's CNSS Standards as requirements that meet the three levels for these two workforce career paths. These six paths (4011-4016) are well understood by many, and could serve very well as an enterprise wide approach. That is the belief of both of the sea services that understand that standards are important and that the NSA IA standards are recognized not only across DoD and also throughout the USG and commercial industry as well. This is the area that this proposal intends to address.

Shown below is a proposed mapping of the two major tracks, plus some additional areas that have been tentatively identified [2]. While this may not be the overall answer that is selected, from a standards perspective, it is a very elegant solution to this new requirement. Thi is because these NSA standards are recognized throughout the Department and some interagency components as well.

Managerial	Required Training
IAM1	4014(E) plus
	4013 (E)
IAM2	4014 (E&I) plus
	4013(E)
IAM3	4014 (E, I & A)
	plus 4013 (E, I)
Technical	
IAT1	4013 (E) or
	4016 (E)
IAT2	4013 (E&I) or
	4016 (E&I)
IAT3	4013 (E, I & A) or
	4016 (E, I & A)

This chart shows the direct correlation between the proposed break out of the tracks with the CNSS Standards. It shows a natural correlation and, if selected, this methodology would make it relatively easy for the services to comply with the directive. The problem is that most of the military IA courses and classes have not been mapped to the CNSS Standards. Furthermore many analysts believe that once they are mapped these curriculums will not cover all the elements to fulfill the entire requirements. Thus most organizations will need some sort of "gap-filler" course that can be integrated with their existing material to bring together a program that uses a blended approach to meeting all the training needs [3].

The synergy of this proposal is that it utilizes courses that are available today in each of the military services and also ensures that the workforce personnel are meeting the stated requirements. To do this, this paper recommends mapping the existing classes to CNSS Standards filling the resultant gaps with web-based options that use Reusable Learning Objects (RLOs) related directly to the approved NSA criteria. Tailored classes would be easily developed for the different Entry (E), Intermediate (I) and Advanced (A) level curriculum as needed, with many different variations permitted.

It has been asked why this proposal suggests the mapping of the new DoD Directive 8570.1 to the existing NSA CNSS Standards (4011-4016) and then mapping CNSS to available federal and commercial training. Why not map to 8570.1 standards? Because in a nutshell, those new federal standards do not exist. Suggestions and proposals have been made by the DIAP and OSD, but there is little logic in creating ANOTHER set of standards, when an interagency group has agreed that the CNSS stanadards are adequate. In addition, who would maintain and update this new database of standards? NSA does an outstanding job of ensuring their standards are maintained

ISBN 1-933510-99-4/05/$15.00

and updated on a regular basis. Therefore in the author's opinion, it is the CNSS and their standards that should be used as a baseline.

This paper proposes a method for mapping and tracking these requirements that the authors believe will be a very viable option for the military services to adopt to meet this requirement. This methodology takes into account not only the courses that are already adopted and in use by the different commands and activities, but it also maps them to CNSS standards for adoption into this process. In addition other capabilities are included such as; the use of pre-testing and review functions to administer on-line training, targeted remedial training, the capability to point students who do not pass to the particular lesson or RLO that could be used to study and retest. These tailored on-line courses could be located on a true web portal that is readily accessible to all service commands without regard to enclave or operational environment. Likewise, this proposal allows the services to reduce their specific classes to only teach military explicit topics that are such as DITSCAP, IAVM, Spillage procedures, etc. Other non-military IA topics previously taught in the classroom that are redundant across all services can be covered by either on-line courses or commercial IA training and security certification courses.

Crse	Service	IAM I	IAM II	IAM III
IASO	Army			
ISSM	Navy			
ISSM	USMC			
IA	USMC			
Crse	**Service**	**IAT I**	**IAT II**	**IAT III**
IASO	Army			
SAS	Army			
SAS	Navy			
SAS	USMC			

To understand how this concept works, the authors have built a rough matrix, based on the IAT and IAM requirements. It shows how the different services have a variety of courses available, but few in fact match to all the needs delineated by the directive. The elements of the CNSS standards that are met by the course are highlighted in yellow, and the gaps or deltas, are noted in red. This, of course, is a draft and as we speak the courses are being mapped using NSA approved software. This will take time, and in fact may be a multi-year effort, but over time the authors believe that eventually all of the major DoD course efforts can be included in this matrix.

What jumps out at even the casual observer is the amount of red or "gaps" in the training. The overwhelming conclusion is that there is a tremendous amount of "red" or non-compliance with the total CNSS IA Standard by these quick sampling of the current ISSM classes. Very few of the military curriculums cover all of the elements of these standards, because their courses tend to be relatively short (weeks to months). This is different than the NSA sponsored university programs which are much more comprehensive and tend to last longer, but also can carry a significant price tag as well as personnel time.

4014	E	I	A
USN ISSM			
USAF ISSM			
USA ISSM			
USMC ISSM			
NSA ISSM			
KARTA			

VI. Available Tools

From this previous discussion, it is apparent that just using existing DoD courses will be insufficient to meet this requirement and that more effort and capability will need to be developed. In addition, a tracking mechanism such as a learning management system (LMS) or learning content management system (LCMS) will be needed as will. This methodology as proposed will involve developing the tools needed to meet the previously described new requirement. The needs will then be matched against a database of training interventions including as many of the following elements as possible:

- The DoD's existing courseware
- Thomson NETg courses
- Thomson NETg Course ILT workbooks
- Karta Courses
- Other vendors, such as $(ISC)^2$ and SANS IA training courses
-

In addition, a major problem that all services have experienced with trying to meet the requirements like 8570 in the past has been that once training needs are determined, it is often difficult to associate needed skills and the appropriate training intervention. Intervention in this context can be a course, book, eLearning, or any other source that delivers the needed information. Currently the DoD has to manually match up the descriptions from the many IA vendors. This painstaking and time-consuming process can impede the delivery of critically needed training. Automated tools such as Thomson NETg's Precision Skilling are now available and can be used to solve this problem and make the matches. These matched competencies and interventions can then be built into a training plan to be managed by the LMS, and possibly the LCMS. The training plan would be composed of the following components, from larger to smaller:

ISBN 1-933510-99-4/05/$15.00 © 2005 IRI/CISSE

- Curriculum - Composed of several courses for example an Information Systems Security Officer Curriculum.
- Course – Composed of several units/lessons. For example, a course could be an eLearning course or a SANS Course.
- Units/Lessons - Parts of course, generally logical groupings of related material. In an eLearning course a unit would be composed of several Reusable Learning Object (RLO).
- Reusable Learning Object (RLO) – The smallest component. An object has a single learning objective and has the course material and assessments internal. This format is generally only available in eLearning.
- The training plan would serve as a template to show the students needed training.

In addition to curriculum development, this methodology also incorporates diagnostic testing at appropriate points. In order to be effective, the eLearning courses diagnostic testing allows the student to further focus on the training the student needed and further reduce the student time. Proposed test products that would interface with the LMS include:

- Tests tailored to the customer's environment
- Tests that would match up with the DoD's internally developed courses.
- Tests that would match up with Thomson NETg/Karta courses, and point to the specific courses needed. For example Karta has some tracks that have multiple courses. A pre-test would point the student to the correct course
- Test to determine whether the student is ready for a commercial certification. These tests would mimic certifications and passing them would be a requirement to actually take the certification test.

VII. Case Study

The following example shows how this methodology could be applied. Davey Jones is an Information Technician (IT) Petty Officer stationed aboard the *USS Kitty Hawk* (CV-63) in the Arabian Sea with additional IA responsibilities. As part of his 5-vector requirements has to attend an IA refresher course, be recertified by the afternoon, as well as run checks on the ship's security settings and implement some new security patches. All in a day's work of course.

Jones starts the configuration changes and in the process of running through the various checks and patch implementations, he notices a configuration that does not seem correct, but he is not certain if it is wrong, or how to correct it if it is wrong. So Petty Officer Jones uses NETg's Search Now query software to find the reusable learning objects needed to teach him how to evaluative configurations. These objects are 5-7 minutes targeted instruction, and eliminate the need to search through manuals or try to find an expert. Jones reviews two objects in ten minutes and is ready to go back and reevaluate the configurations. After completing his test work and grabbing a bite to eat lunch, Jones must now attend his refresher course on DoD IA standards. He has previously taken both NETg and DoD developed CBT pre-requisite courses. His records have been automatically updated to show this pre-training and that he is prepared for the hands-on training that he will receive. This hands-on course is thus now only four hours long as the prerequisite courses have eliminated the parts of the course that does not require an instructor. A happy Davey Jones only spends four hours in classroom learning how to apply IA procedures on the ship. At the end of the course the instructor grades him. This information is then input to the LMS to update his training records. His updated records are transferred to the DoD's central LMS at his time or updated when the ship returns to port. His records now reflect that, when he returns to port, he is qualified for advanced hands-on training given by $(ISC)^2$

The critical success factors of this case study include:

- Management receives continuous metrics on student progress and completions.
- Students do not proceed to the next step without successful completion of prior steps, although the resources used for the training would continuously be available for performance support.
- Media based training, including eLearning and books, is used when possible.
- Instructors and off site classes are used where their expertise can make a difference.

VIII. Benefits of this Methodology

In the opinions of the authors, there are many benefits to this proposed methodology for meeting the requirements of DoD 8570.1-M. A few are shown below:

- Existing training is mapped to needed competencies; ensuring training is relevant to the job.
- Mapping training makes the best use of available resources and shows what new training must be developed or outsourced.
- Career path planning guides student steps to increase their professional knowledge, increasing job performance and retention.

ISBN 1-933510-99-4/05/$15.00 © 2005 IRI/CISSE

- The most cost-effective methods used when applicable, increasing funds available for hands-on training.
- High level diagnostic testing directs students to the right learning events, thus avoiding subject areas where they are already competent.
- Course level pre-tests ensure learner is only presented what they need to know.
- Post-tests ensure learners have mastered subjects thereby ensuring they are qualified for next steps and for certification tests.
- Instructors are used where are most beneficial, thereby increasing student throughput from the same number of instructors.
- Use of pre-work allows students to train when they are in isolated environments, such as on shipboard.
- Electronic resources (eLearning and online books) are available as performance support for employees.
- Performance is being tracked throughout the process thus making management reporting sand metrics available.

IX. Summary

The proposed methodology as stated in this paper can be delivered now. It optimizes the training already developed by the services. It allows them to maximize their sunk costs and still meet the requirements of the new directive by only paying for the additional learning modules needed. Every DoD course can be mapped and plotted against the needed standards, thus giving managers a graphic display of any gaps or additional training that is required.

This is not a futuristic dream. The components listed below are already in place and are being used by customers, although not as integrated as proposed in this package:

- Competency development
- Role based training and certifications matched to the clients needs
- Comprehensive diagnostic testing
- Comprehensive set of blended learning resources
- Performance support capabilities
- Transparent student tracking
- Metrics tracked by the LMS.
- Soft skill training

As we speak, the authors are currently working with their DoD clients to deliver pilot programs of this proposal with the four services to demonstrate the capabilities of this methodology over an enterprise-wide architecture. Early results are positive, and we believe that if adopted across the DoD, this process will go a long way toward solving the requirements laid on by this directive as well as strengthening the military's networks and posture for the future.

X. References

[1] Department of Defense (DoD) Directive 8570.1 *Information Assurance Training, Certification, and Workforce Management*, 15 August 2004.

[2] Discussion with Steve Busch, DoD Information Assurance Program, 18 October 2004, Quantico, VA.

[3] Discussion with Mike Knight, Naval Network Warfare Command, 6 February 2005, Philadelphia, PA.

ISBN 1-933510-99-4/05/$15.00 © 2005 IRI/CISSE