Information Assurance Workforce Improvement Program (IAWIP) Implementation for Cybersecurity Convergence Group(CCG)

Chanakya Gaur

EN.650.653.01 – Financial Issues in Managing a Secure Operation

Information Security Institute, Johns Hopkins University

12.1 Assume that you have just been hired as the Chief Information Security Officer (CISO) for the Smith, Barrett, Jones, and Darby (SBJ&D) Cybersecurity Convergence Group (CCG)1 and your first task as CISO is to consider all or specific parts of the DoD 8570.01-M, IAWIP for implementation at the CCG. What 8570.01-M components will you recommend for adoption at SBJ&D CCG? Why did you select specific components while leaving others out? Are there IAWIP-related components that you added that were not in 8579.01-M? If so, what were they and why did you add them? Your paper will be sent as a read ahead for the Board of Directors and Senior Partnership Group for the annual SBJ&D CCG Security Conference in New Zealand next month. Good Luck.

Introduction

The Information Assurance Workforce Improvement Program is a DoD directive that requires all professionals who conduct information assurance functions to obtain specific certifications according to their job. This directive applies to contractors working with the DoD for information assurance as well. The directive is explained with a manual DoD 8570.1-M which guides the implementation of the Information Assurance Workforce Improvement Program. The directive of this program provides an organization-wide solution to certify, train and manage the Information Assurance Workforce professionals according to their job functions so they have relevant training. The goal of this program is to eventually generate sustainable skilled workforce which would prevent and respond against security attacks against systems, infrastructure and information. The information assurance workforce are professionals who either require privileged access to a computing, network or enclave environment or have the responsibility of managing information security for them[1]. In this report, we shall discuss the guidelines provided by the DoD 8570.1 for maintaining a knowledgeable, trained and certified workforce which would be able to combat the necessary security risks at different roles in the organization and choose the guidelines that would be ideal for the Cybersecurity Convergence Group to implement for their organization.

Keywords: IAWIP, Training, Certification, Information Assurance, DoD

---

[1] 8570.01 - GovITwiki. (2018). Govitwiki.com. Retrieved 30 April 2018, from http://govitwiki.com/wiki/8570.01

Components of IAWIP

Workforce Structure[2]

The information assurance program focuses on the development, management, operation and management of security for systems and networks of the DoD. Professionals involved with information assurance functions have been assigned duties that they need to perform and requirements that they need to adhere to by this directive. The manual also explains that the requirement for certifications in the program is so that personnel have "a baseline understanding of the fundamental IA principles and practices related to the functions of their assigned position"[3] and that meeting requirements with a combination of formal training and on-the-job training would be a requirement. These professionals are expected to work closely with data owners and the information systems so that they can secure its use and operations. Given the sensitivity of the work expected from the workforce, the application process is rigorous, involving policies, principles and practices of the information technology services. They are expected to setup authentication systems, monitor software and hardware and look out for vulnerabilities, security anomalies or system weaknesses. The workforce is also required to review audit information to detect any system abuses. They are also expected to patch i.e. assess and implement the identified corrections as directed by the Information Assurance Vulnerability Management directive.

The program consists of various roles and functions that need to be carried out, which is why the workforce has been divided into categories. The categories describe the experience, training and certifications and clearance required from the personnel. The manual has divided the information assurance workforce into the following categories: Information Assurance(IA) Technical workforce and

---

[2] DoD Directive 8570.01 - Frequently Asked Questions. (2018). Iase.disa.mil. Retrieved 2 May 2018, from https://iase.disa.mil/iawip/Pages/iaetafaq.aspx

3 Department of Defense Directive 8570.1. (2005). Information Assurance Workforce Improvement Program Incorporating Change 4, 11/10/2015 December 19.

IA Management workforce. Additional specialty groups are the Computer Network Defense Service Providers (CND-SP) and IA System Architects and Engineers(IASAEs). These groups are additionally subdivided into categories depending upon the functional skill requirement and the system environment they focus on. Every IA position at the DoD belongs to a category and the personnel must complete requirements to continue at the position.

Technical Workforce Overview

The personnel required to perform all technical aspects of information assurance at any level are a part of the technical workforce (IAT). The position of the IAT establishes the certification and training requirement of the personnel. These categories of the technical workforce are cumulative i.e. the personnel any level must also have completed requirements of the preceding levels. Training requirements of the technical workforce include participation in initial training before or immediately on assignment of IA responsibilities which should be sufficient to make the individual competent for the role and satisfy the certification requirements specified by the manual. The individual should also complete an evaluation which would be practical and consist of on-the-job skills to continue training to maintain certification and must contribute 120 hours over a period of 3 years.

The IAT personnel category comprises of[4]:

- Level 1

  The IAT Level 1 personnel work with the computing environment and make it less vulnerable by implementing IAT controls and patching vulnerabilities of the operational systems of the organization. The functions of IAT Level 1 are to identify security violations and generate reports of the incidents to mitigate adverse impacts, to apply policy and pre-

[4] Summary of Cyber Workforce Qualification Requirements. (2018). Iase.disa.mil. Retrieved 2 May 2018, from https://iase.disa.mil/iawip/Pages/summary_wf_requirements.aspx

established guidelines in the operational systems and provide end user support. Their functions also include installation of control measure, password policies and upgrading pre-installed software. Level 1 IAT should also participate in vulnerability assessment and conduct IA tests to ensure the safety of the systems. To be competent to perform these functions effectively, the manual states that personnel should have 0-5 years of experience, have a baseline certification and OS certificate and should have a basic knowledge of information assurance concepts and practices. Level 1 IAT usually report to an IAT manager.

- Level 2

  The IAT Level 2 personnel work at the network environment and advanced computing environment level. Their focus is on intrusion detection, discovering and patching vulnerabilities and securing remote access points which will ensure improved security of systems. The main function of Level 2 personnel is to be proficient with the computing environment, ensure that there is no policy violation in the network environment and provide end-user support for all IA related applications on the network environment level. The requirements for personnel to execute these jobs efficiently include having more than 3 years of experience in a related field, necessary certifications and OS certificate and should be proficient with Level 1 technologies. Level 2 IAT professionals usually report to the NE manager.

- Level 3

  The IAT Level 3 personnel work at the enclave environment level which includes monitoring, support, testing and troubleshoot software and hardware related to all CE, NE and enclave environments. The level 3 personnel are expected to have proficiency in all levels of IAT. The focus of Level 3 personnel is to recommend, schedule and implement IA solutions within the environment and provide support of all environments. They are also expected to implement operational structures, provide support to system developers regarding vulnerabilities and evaluate performance of functional operations. The requirements for these

professionals include experience of a minimum of 7 years, ability to work independently and lead others, be a U.S. citizen and have the necessary certifications. Level 3 professionals usually report to the enclave manager.

Workforce Management Overview

The personnel required to perform the managerial functions of the organization are a part of the information assurance management (IAM) workforce. The IAM personnel, whether or not they directly perform IA functions, they are required to have the certifications and training required for the functions of the position. These professionals are required to have management as well as technical trainings and certifications to ensure effective performance. The IAM comprises of Levels 1 2 and 3 which are required to perform IAM responsibilities.

- Level 1

  The IAM level 1 personnel work towards implementing and operating DoD information systems and components within the computing environment. Their focus is to use government publications to govern systems and administer the environment. The professionals working at this level are usually required to complete initial certifications, have 0-5 years of management experience and must be capable to manage IA operations of CE.

- Level 2

  The IAM Level 2 personnel work within the Network environment, performing security related tasks such as development and implementation of security standards and procedures. They ensure the secure functionality within the NE by developing, implementing and enforcing policies according to the legislature. Their work also includes developing plans and generating guidelines regarding security of the environment. These personnel are required to have a minimum of 5 years of management experience, required certifications and baseline certifications.

- Level 3

  The IAM Level 3 personnel ensure security and functionality of all enclaves. They develop security standards and procedures through the DoD certification and accreditation process. These professionals are required to be U.S. citizens, with a minimum experience of 10 years, should be able to apply knowledge of IA policy, procedures, and workforce structure to develop, implement, and maintain a secure enclave environment.

Implementation Suggestions for CCG

The directives provided in the manual, as we can see are well justified and implementing them would ensure a capable workforce. However, I believe that the directives cannot be followed directly and should be modified according to the CCG's needs. Following is a list of comments for implementation for CCG divided by categories[5].

- Initial Training[6]

  According to the guidelines, the in-class training and the on-the-job training is required. This is necessary for all workforce working with information assurance as it prepares them for efficient performance. Additionally, I shall also want to point out that the training should be intensive initially so that there are less resources required for continuous learning. There could possibly be an in-house certification or test in which their preparedness for the job could be tested. The ideology behind this proposed change is to thoroughly prepare the workforce so that errors during work are minimized and future training is easier.

- Certification

---

[5] DoD Approved 8570 Baseline Certifications. (2018). Iase.disa.mil. Retrieved 2 May 2018, from https://iase.disa.mil/iawip/Pages/iabaseline.aspx

[6] Turk, R. W. (2013). Preparing a Cyber Security Workforce for the 21st Century. ARMY WAR COLLEGE CARLISLE BARRACKS PA.

The manual has provided a list of certifications suggested for the workforce at different levels. These certifications need not be compulsory for the workforce to complete if they can prove that they have the knowledge that the certification imparts. As an organization, having a large number of personnel complete certifications would cost the organization a lot of money. As a policy, the organization can conduct exams to evaluate the level of knowledge some personnel has and below a cut-off score, make completing the certification compulsory. The cut-off can be held at a high standard to ensure quality of workforce.

- Continuous Education[7]

  In the field of security, continuous education is very important there are new concerns and mitigation techniques developed daily. According to the manual, the workforce should invest 120 hours in continuous education over a period of 3 years or 40 hours over a year. However, these continuous education timeframes are too big when compared to the pace at which the industry is growing. Follow-up trainings and certifications should be held more frequently, probably quarterly and their duration could be shortened so that there is no major loss of work time. According to me, there should be 10-hour trainings every quarter to ensure that the workforce is up-to-date.

- Background Investigation[8]

  The manual specifies a variety of background checks that need to be performed before allowing any personnel in the IA workforce. This guideline should be strictly followed to reduce the possibility of insider attacks and securing the organization from within. Additionally, it improves the reputation of the organization and gives its clients a sense of

---

[7] Winter, R. L. (2010). Redesigning the Information Assurance Undergraduate Curriculum at Regis University.

[8] What Types of Background Checks Are There? | CriminalWatchDog. (2018). CriminalWatchDog. Retrieved 2 May 2018, from https://www.criminalwatchdog.com/faq/types-of-background-checks

added security. Additionally, a requirement for U.S. citizenship need not be a requirement unless its government related work.

- Experience

  I believe that the experience guidelines, although necessary, need not be strictly followed. The emphasis of selecting workforce should be focused on the knowledge they have and their achievements. Experience cannot be overlooked, but at the same time it should not be a major factor for selection. Professionals who have less experience would be ideally more inclined to learn and develop themselves more, would have a higher efficiency and could be guided as required.

These suggestions, I believe would be more inclined towards the requirement of the CCG. The modifications focus on saving resources for the organization without compromising the quality of the workforce.

Conclusion

From the Information Assurance Workforce Improvement Program directive and the manual, we have received information insight into managing the workforce in an efficient and organized manner. The levels and categories help us to categories work roles and requirements accordingly. However, the suggestions mentioned in the report can be used to save on to resources and not compromise on the quality of the workforce. We can also minimize risk at the workforce level for internal security. This report has evaluated the guidelines and suggested the guidelines that should be adopted and the ones which need not be.