Determining the Role of the IA/Security Engineer

Brian Dutcher

Determining the Role of the IA/Security Engineer

GIAC (GSLC) Gold Certification

Author: Brian Dutcher MSIA, CISSP, GSLC, Security+, PMP, bdutcher.ia@gmail.com
Advisor: Rick Wanner

Accepted: March 15, 2010

Abstract

Within the information technology fields, the term "engineer" has become generalized and has lost its true meaning. This is also the case for the more specialized security or information assurance (IA) engineer. This generalization has resulted in a myriad of positions labeled "engineer" but with no real substance.

The objective of this paper is to identify and determine what a security or information assurance engineer really is and their role in the organization. It will provide managers with the necessary background information to determine the need for an IA Engineer along with the technical and professional requirements required to fill such a position. The manager will gain an understanding for the proper utilization of the security engineer within their organization, and the benefits of staffing this position with properly trained and qualified personnel.

1. Introduction

What is your view of the role performed by an IA/Security Engineer? Is it focused on securing the network perimeter through the operations of the firewall, virtual private networks (VPNs), intrusion detection system/intrusion prevention system (IDS/IPS), network access control (NAC), data loss prevention (DLP) and enterprise anti-virus solutions? Is it the network specialist responsible for the secure design of the local area network (LAN), virtual LAN (VLAN), wide area network (WAN) and all endpoints? Is it the systems designer or operator responsible for the security of all clients and servers? Is it a software developer specializing in developing and hardening custom applications? Is the IA/Security Engineer someone who is an expert in all these areas? Is the IA/Security Engineer a specialized single technology (i.e. Cisco) expert, or is the position technologically agnostic, working at a higher level where specific detailed technology is irrelevant in the bigger scheme of things?

Depending on one's background, experience, and job sector, the description and definition of the roles, functions and responsibilities of an IA/Security Engineer will vary. This would be expected from individuals outside of the IA career field, but this is also true for those of us specializing in the IA career field, as it is a poorly defined position. The IA/Security Engineer has the ability and responsibility to ensure security is built into the solution/design as part of the foundation. Their job is not to apply the "ACME" Security sticker as a wrapper and call it secure. This paper explores and examines the way the IA/Security Engineer is utilized within the public and government/DoD sectors. It will document the results of an online survey which captured the way this position is currently defined by our cohorts. It compares it to a more well-known and universally accepted engineer, the Professional Engineer (PE). How the organization can benefit from the proper use of the position is also covered.

2. The Current Information Assurance Workforce

Today's information assurance (IA) workforce is as diverse as ever, and has the daunting challenge of ensuring complete security of the organization's intellectual property, critical infrastructure, and in some cases facilities and personnel. Achieving this while keeping up with the dizzying pace of new information technology (IT), IA technology and all of the associated specialty niches that include the accompanying vulnerabilities and threats, has created a very broad and unique career field. To realize this, all one has to do is examine a handful of

organizations; public, private, government, and DoD, to discover a litany of position titles and responsibilities.

Overall, one has to realize that the IA workforce and its development of IA professionals are still in its infancy. Using the Carlson, Burgess and Miller timeline, the Colossus vacuum tube computer that was operational at Bletchly Park in 1943 or the UNIVAC that was in operations in the U.S. in 1951 can be used as a starting point (p. 15, 21). In this regard, modern computing has been taking place for approximately 60 years. The mainframes of the 50, 60 and even 70s were primarily concerned with physical security, not the IA-Triad. This was due to the sheer size, cost and complexity of the systems with little to no connectivity that was operated by a small group of highly trained staff.

For the majority of organizations, the IA workforce is a descendent and specialty of the IT workforce which could have its origins as far back as the mainframe shop. The IA career field is a relatively young subset of the overall IT career field, the result of which creates an environment where the career field itself is being defined by individual organizations in the public, private, academic, government, and DoD sectors. Depending on the size and scope of the organization, the IA workforce can be broken down into two overarching categories, general and specialized.

The infancy of the IA career field is demonstrated in several ways. First, it wasn't until April 1985 that the National Computer Security Center published the first book (Green Book) in the Rainbow Series. The Green Book (CSC-STD-002-85) was only focused on DoD password management, a very small attribute under the overall IA umbrella (FAS, 2006). The first CISSP exam, what is considered the bedrock of IA credentials was not given until 1994 (ISC^2, 2010). The first GIAC certifications were not awarded until February 2000 (GIAC, 2010). Naraine states that US-CERT, which was created to improve the computer security preparedness and response to cyber attacks in the U.S., was not established until September 2003. These four are used as reference points because they have formed the guiding IA principles used today. When you consider your bedrock foundational IA organizations are 25 years or younger when compared to a 60 year plus industry, the infancy clearly stands out.

2.1. The General IA Workforce

The general IA workforce is those individuals in positions that require a great deal of breadth in terms of skills and knowledge. Commonly these individuals are responsible for

everything from the firewall and anti-virus solution to physical security and incident response to security architecture. You can think of them as the jack of all trades, master of none, security generalist and IA point man. These positions are very similar to the small IT shop, all-in-one IT position, the Swiss Army knife of IT. It is common for these types of positions to develop out of necessity from small IT shops and can even form small (five or fewer) IA shops.

The general IA workforce and the entire IA workforce both benefit from having organizations such as SANS, ISC2 and ISACA, provide vendor neutral broad overarching IA certifications. These three organizations provide broad IA certifications, example include the GIAC Security Leadership Certification (GSLC), the ISC2 Certified Information Systems Security Professional (CISSP), and the ISACA Certified Information Security Manager (CISM).

2.2. The Specialized IA Workforce

The specialized IA workforce is generally seen in larger organizations that have more complex security needs and the resources to have dedicated and specialized IA positions. Another source of specialized IA personnel is consultants that provide services for hire. In both instances, we see unique specialties such as firewall and IDS/IPS administrators, incident responders with specialized forensic skills, red and blue team penetration testers, audit/event log analysts, IA managers and the elusive IA engineer.

The specialty IA fields also benefit from similar specialty IA certifications such as the GIAC Certified Forensics Analyst (GCFA), the GIAC Certified Penetration Tester (GPEN), and the ISACA Certified Information Systems Auditor (CISA). However, there seems to be one IA specialty for which a certification truly does not exist, the IA Engineer. The IA Engineer is an IA specialty so unique that most organizations have their own definition of the roles duties and responsibilities.

2.3. The IA /Security Engineer

The IA/Security Engineer is a mysterious position, everyone seems to know one, but nobody can actually define one. The position itself suffers from three levels of immaturity. First, the IT field itself is young; we'll call it the college student. The IA specialty field would be even younger, let's say high school student. Well, the IA/Security Engineer is more like the middle school seventh grader with a squeaky voice. Geeky, awkward, and nobody really knows what they are capable of or what to do with them, just kind of left in their small unique misunderstood group.

Because of this misunderstanding, most organizations are assigning personnel to positions as "engineers" when in fact they are nothing more than technicians, administrators and operators. When someone sees "CPA", they link it to an accountant. If you see "MD", you link it to a medical doctor. The other engineering disciplines, Electrical Engineer (EE), Chemical Engineer (CE), Mechanical Engineer (ME), etc are all recognized and linked to a specialty. When someone sees the title IA Engineer, Cyber Security Engineer, or the mystic Information Assurance Systems Architecture Engineer (IASAE) they pause and are not sure what to think. It is as if anything related to security that is perceived as technical or difficult by management is grouped under the umbrella term IA/Security Engineer.

But there is much more to it than that. The true IA/Security Engineer is responsible for designing, developing and deploying security related systems and security in systems. Their responsibilities and skills can be very specific such as designing a hardware security appliance or security software. The IA/Security Engineer could be a hired consultant responsible for designing and implementing a secure system for a client. Although the IA/Security Engineer could work in many different areas across the organizations IT spectrum, they are predominately focused on the core principles of ensuring the confidentiality of the data, integrity of the data and the system, and availability of the data and the system. The IA/Security Engineer ensures these core and integral components are implemented throughout the systems and data's lifecycle, from design to decommission.

3. Today's IA/Security Engineer

The IA Engineer of today is as diverse as the IA career field. It seems to be the most common form of IA or cyber security position. Is this because the duties and tasks executed by the IA profession are so misunderstood that managers and human resource departments' just randomly assign the term "engineer" to any technical position not fully understood? In the true context of the word, the term "engineer" means more than what HR departments have carelessly applied to job titles and position descriptions. Engineer is more than a technical word; it is the description of a professional who possesses a specialized set of skills based upon a common body of knowledge that has been validated by a recognized governing and or licensing body. In this context, there are very few true engineers working in the IA career field.

For example, using a web job engine to search for the term "security engineer" returns a multitude of unique positions. From the searches conducted, the following were the most common job titles listed;

- Application security engineer
- Biometrics security engineer
- CISCO, Checkpoint, iPhone, Symantec, McAfee, security engineer
- Communications technology security engineer
- Cyber security engineer
- Data security engineer
- IA security engineer
- Info Sys Security engineer
- Information security engineer
- IT security engineer
- Network security engineer
- Software security engineer
- Systems security engineer
- Web application security engineer
- Web portal security engineer
- Web security engineer
- Windows information security engineer
- Wireless security engineer

This broad spectrum of defining what an IA engineer is and does was also captured in an online survey conducted as part of this research through www.surveymonkey.com. In all, 72% of respondents reported that an IA engineer position existed in their organization and 4% reported the position did not currently exist but there are plans to create one (Table 1). Of these respondents, 71% indicated that their organization had one or more IA engineers on staff filling an identified position (Table 2). The true uniqueness of this position is clearly evident in the results from the number of IA engineers on staff in existing positions question. The low was zero while the high was 1500, the median was three and the mode was two IA engineers per organization. This broad range of results between organizations leads to a hypothesis that there are definitely differing descriptions of what the IA/Security Engineer role encompasses.

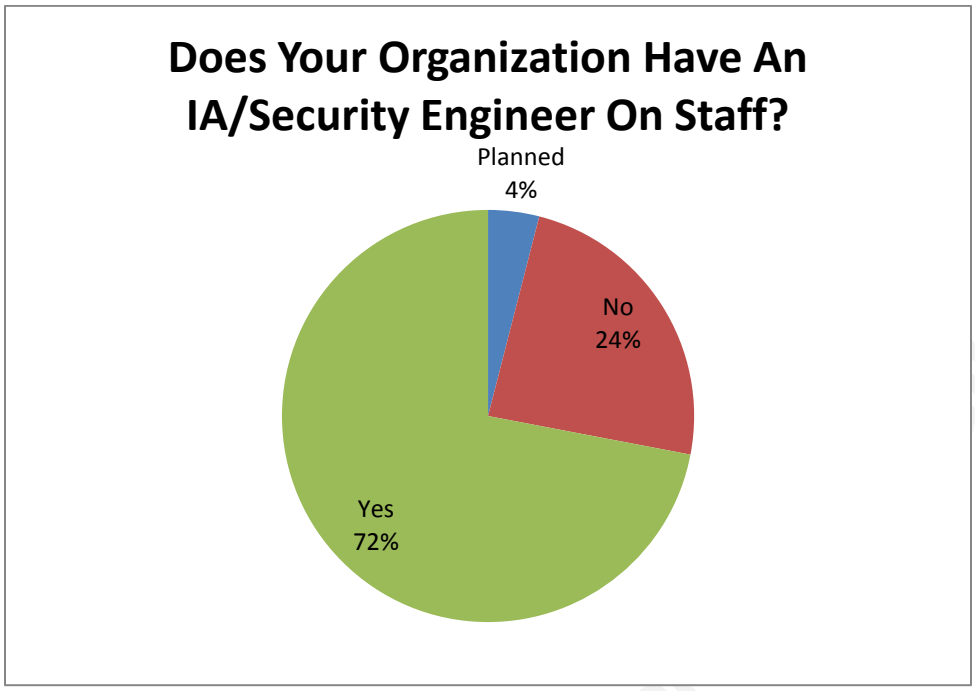

Table 1

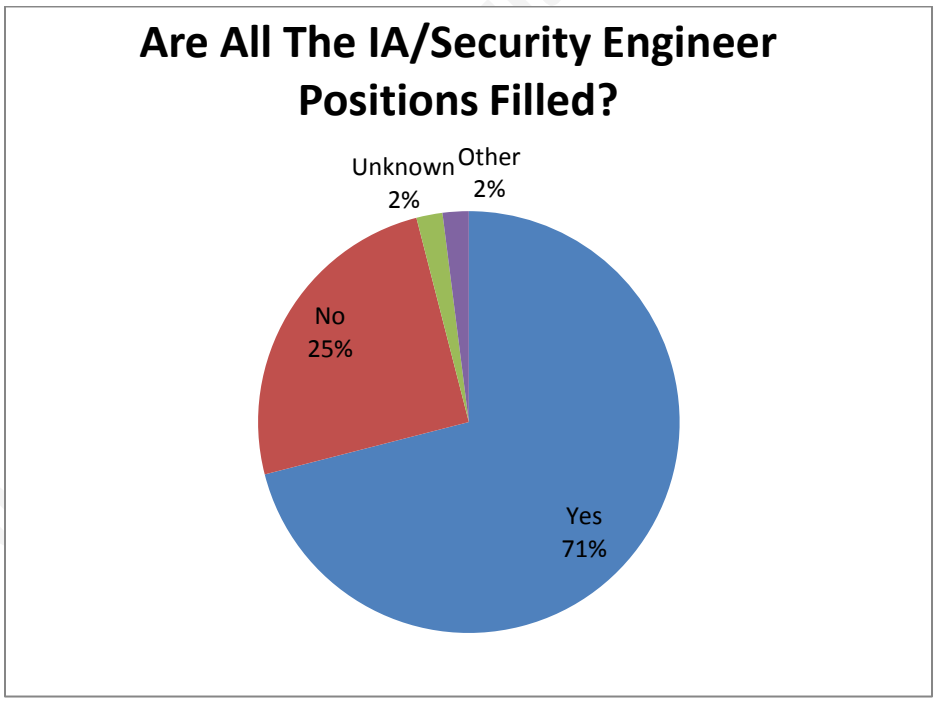

Table 2

Using the common perception, one may generally think of an engineer as an intelligent, well educated individual with at least a 4-year college degree based heavily on mathematics and

some type of certification or license to provide proof their skills have been evaluated. However, the survey also highlighted that there are vast differences in education requirements for the IA/Security Engineer. The responses in each category indicated that a degree was either required or "preferred"; 3% responded with an Associate degree, 73% responded with a Bachelor degree, 8% responded with a Masters degree and 16% responded that no degree was required (Table 3).

Perception and reality further separate when looking at the results for the survey question on whether or not an IA/security certification was required. One would expect that if an organization was not requiring a college education that could be substituted with x-years of experience for an engineering position, that they would require at least one of the recognized IA/security certifications. The surprise in these results was no, that is not the case. The results (see Table 4) were that 66% of organizations required some level of certification but that 31% did not require any level of certification. For the remaining 3%, these organizations encouraged, but did not require certification. Another interesting finding from the certification requirement results was the actual certifications that were listed as required or preferred (note that many responses had multiple certification options). The ISC^2 CISSP had the most responses followed by GIAC (no specific certification reported) and ISACA. What is even more interesting is that none of these organizations offer an IA/Security Engineer certification, with ISACAs certification offerings being the furthest from an IA Engineer.

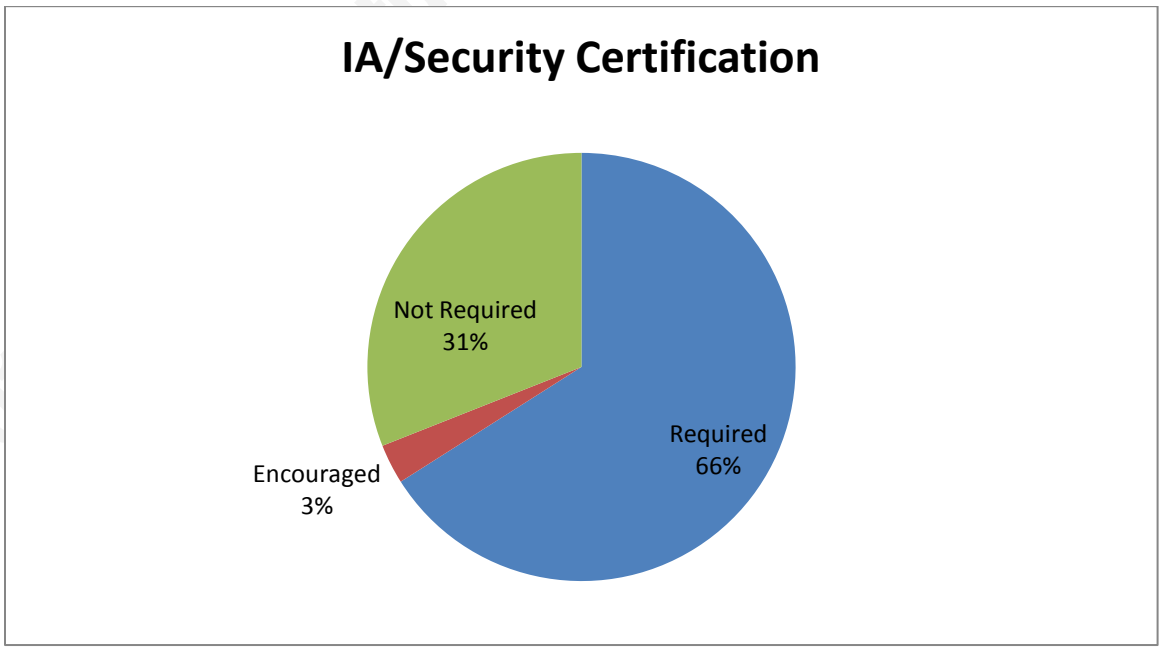

Table 3

Brian Dutcher, bdutcher.ia@gmail.com

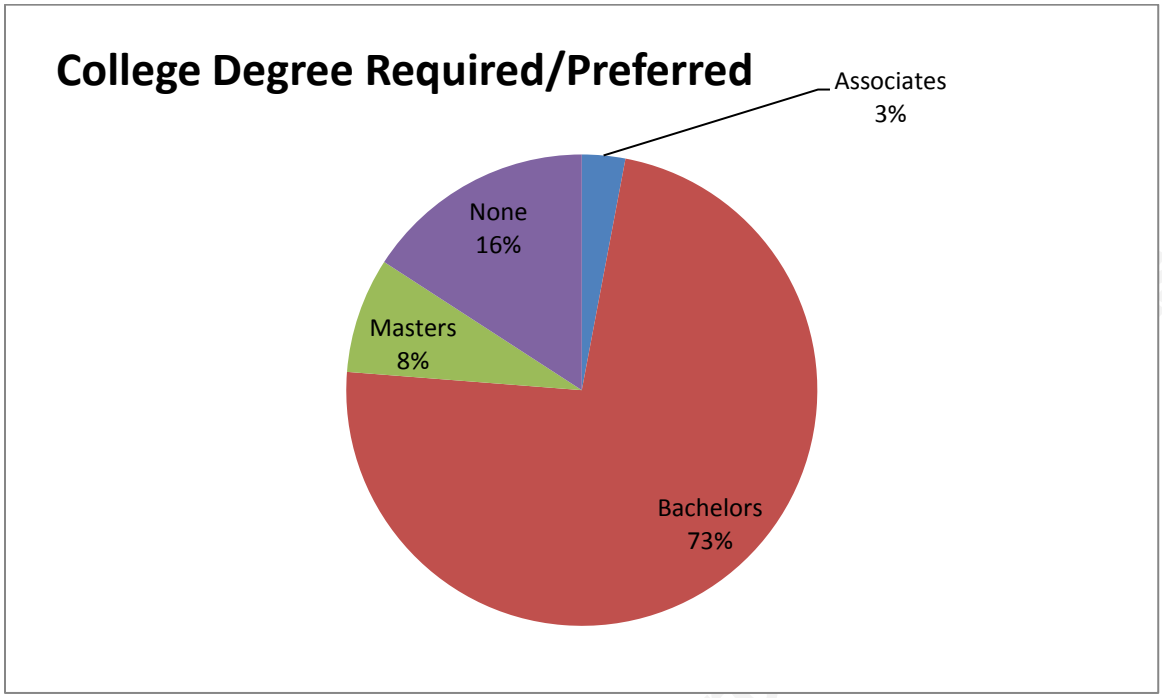

Table 4

One question on the survey though leads to the conclusion that even though formal college education and IA/security certifications are not required, a higher level of job related experience is required. As Table 5 illustrates, 58% of the respondents indicated that the positions required greater than three years experience (3-5 Years 22%, 5-7 Years 36%). This was followed by responses in the opposing areas of none (11%), 1-3 Years (8%), and 7-10 Years (8%). The remaining 14% were responses outside of these categories.

Brian Dutcher, bdutcher.ia@gmail.com

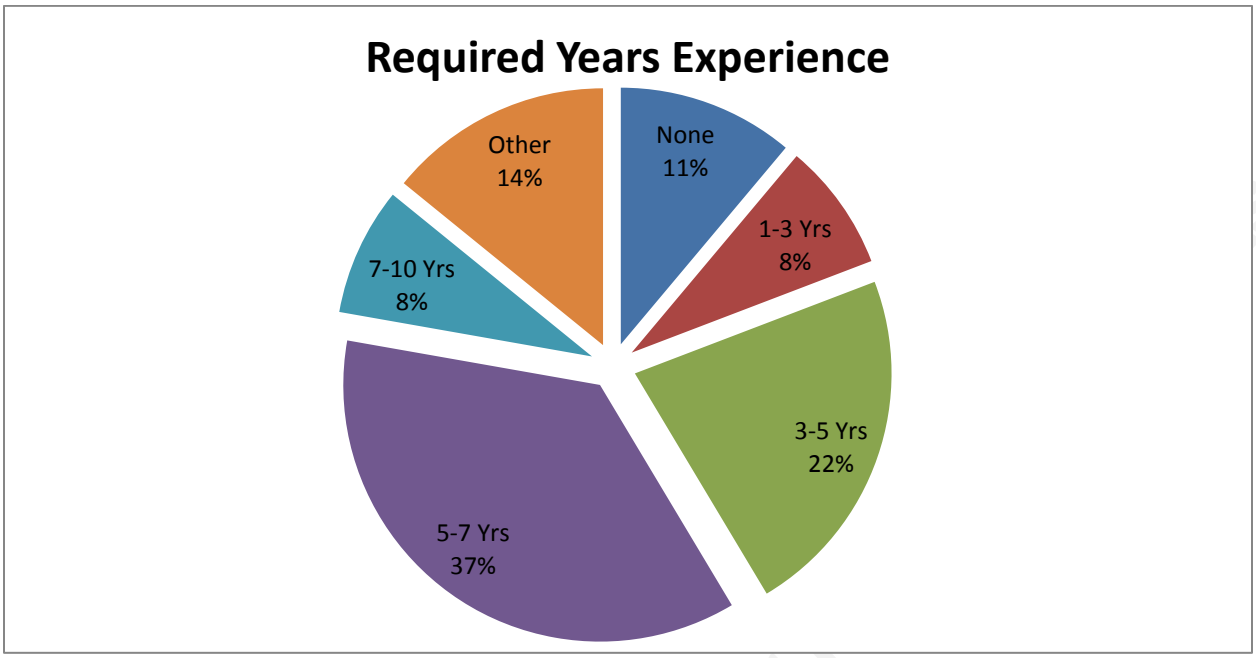

Table 5

However, the reader must remember that these are non scientific survey results and this is only a high level examination of the position. Every sector whether commercial/public or DoD/Government, will have a different and unique perspective on exactly what this position is, the duties performed and the benefit that it brings to the organization.

3.1. Commercial/Public Sector Interpretation of the IA/Security Engineer

As mentioned prior, the commercial and public sector has established a very broad spectrum of duties associated with the IA/Security Engineer. These very broad and essentially catch-all job descriptions are as unique as every organization and equate to performing any number of security related and general IT type tasks. The results of the survey and several online IA/Security Engineer job descriptions once again demonstrated this.

The most common theme across all the responses and online job postings is that in the commercial/public sector, the IA/Security Engineer is actually IA/Security Operations. Many of the jobs being described are really technicians, administrators and analysts. If they were in another discipline of IT, i.e. server administrator, database administrator, they would not be labeled as engineers. There again, it can be the unintended ignorance of human resource departments as to what the positions actually do and how they should be labeled. The following

duties/assigned tasks and responsibilities are a summary of all those listed from the survey and online job posting that are not true IA/Security Engineering tasks.

- Perform security tool administration providing risk analysis of the following:
  - Vulnerability scanners
  - Security event logging & monitoring analyzers
  - Intrusion Detection/Prevention System (IDS/IPS) and firewall logs
  - Performs system and network security audits
  - Anti-virus products and central console
- Perform the day to day operations, management and administration to protect the integrity, confidentiality, and availability of information assets and technology infrastructures of the organization:
  - IDS/IPS
  - Firewalls
  - Anti-virus
  - Event log analysis
  - Perform threat, vulnerability, and risk assessments
  - Manage/perform security audits
  - Develop security awareness instructional material
  - Perform or assist with investigations
  - Coordinates the handling and resolution of incidents of security breach
- Day-to-day operations and maintenance of computer facilities and IT resources including network support, server support, desk top support, and telecommunications services

As bad as this may sound to some, not all is bleak for the IA/Security Engineer position. Although there was not one position that contained engineering-only tasks, there were positions that included several engineering tasks, some upwards of 80%. A summary of the IA/security engineering duties and responsibilities listed from the survey responses and the online job postings are included in the following list.

- Provides analytical and technical security recommendations to other team members, oversight boards, and clients. Identifies requirements, based upon need or as the result of a security issue that puts organizations systems at risk.
- Meets with clients and management to help specify and negotiate application security requirements, reviews current policies and procedures for applicability, and system OS security patch levels, and ensures safe transition of applications to production.
- Develops technology to automate security monitoring
- Develop, debug, test and support the certification process
- Create, maintain, and document security baselines
- Evaluate and recommend secure remote configurations

- Active member in technical workgroups to recommend effective security configurations and architecture
- Liaison to the Enterprise Architect, WAN, LAN, and Enterprise Management Teams to effectively communicate and architect security solutions
- Develops documentation to support ongoing security systems operations, maintenance and specific problem resolution.
- Works with and coordinates appropriate IT staff to implement solutions which will meet or exceed customer expectations
- Provide risk analysis for vulnerabilities, incidents and change requests
- Functions as technical lead during a security incident response

3.2. DoD Description and Role of the IA/Security Engineer

As one might expect, the U.S. Department of Defense (DoD) has the IA Engineer position fairly well defined and documented in a formal publication, DoD 8570.01M Information Assurance Workforce Improvement Program. This publication provides overarching guidance to all the Services and DoD Components establishing a minimum baseline allowing each Service and DoD Component to establish more refined, but not less stringent, requirements that fulfill their mission and requirements. (ASD(NII)/DoD CIO, 2010)

The DoD labels the IA/Security Engineer position as an IA Systems Architect and Engineer (IASAE). DoD 8570.01M (2010) outlines the role which can be fulfilled by military, government civilian, or contractor, to include local nationals in some situations (p. 60). One unique aspect of the way the DoD 8570.01M defines the IASAE is that it does not have to be your duty title or even your primary duty. The act of performing IA engineering tasks (which are defined below) classifies you as an IA Engineer and subsequently applies all the requirements (see section 3.3.2) to perform the tasks (p. 61). DoD 8570.01M also defines the IASAE position as a Level I, II, or III; each having greater authority and subsequently greater requirements (p. 60-71).

DoD 8570.01M assigns the IASAE positions as being responsible for the design, development, implementation, and/or integration of a DoD IA architecture, system, or system component for use within the computing environment, network environment, and/or enclave environment. Incumbents ensure that IA related information systems will be functional and secure within the computing and networking environments. They will also ensure that the architecture and design of DoD information systems are functional and secure. This may include designs for program of record systems and special purpose environments with platform IT

interconnectivity. Incumbents may also be responsible for system or network designs that encompass multiple computing and/or network environments to include those with differing data protection/classification requirements (p. 62, 65, 68). See Appendix A for the full list of functions/tasks performed by each level of IASAE as identified by DoD 8570.01M Change 2 dated April 20, 2010.

As defined and detailed as the IASAE is in the current version of DoD 8570.01M, the entire IASAE chapter is being rewritten. The draft rewrite does not degrade or remove any of the IASAE functions or roles; in fact the chapter expands to address the shortfalls of the current publication. Some of these shortfalls include the lack of identifying the IASAE roles across the DoD 5000 Acquisition Model, the System Development Life Cycle and the Risk Management framework (DoD 8570.01M Chapter 10 Rewrite Draft, 2010). By aligning the roles across these frameworks, it allows the tasks to become more specific to each level of IASAE. Examples of this realignment include concepts and capabilities, versus design and develop versus integration/testing and operations and maintenance. Also addressed, is the current lack of an IA Software Engineer role. This addition will provide the framework to ensure security is considered and designed in from concept to code to operational deployment.

Survey responses that were from the DoD for the most part followed in line with DoD 8570.01M for tasks being performed. Compliance verification of Defense Information Systems Agency (DISA) Secure Technical Implementation Guides (STIGs), Service security alerts and bulletins, and DISA/DoD standards were common among responses. It was also interesting that even in the DoD, the most common application of the IASAE is in operations. Performing general INFOSEC functions by IA technicians to ensure the Service/Components information systems data availability, integrity, and confidentiality, and non-repudiation was very common.

As one can see, the DoD has developed overarching guidance to all the services and components a description of the IASAE and their role in the organization. This is very important in maintaining the positions function, role and integrity across the hundreds of locations and programs around the world. The DoDs attempt was absolutely necessary in managing this diverse position across a global enterprise.

3.3. IA/Security Engineer Position Requirements

While the description of and roles performed by an IA/Security Engineer define the position, the minimum education, experience, and certification requirements are what really

shape the position and determine it capabilities. The next two sections outline these requirements for the commercial/public and DoD sectors.

3.3.1. Commercial/Public Sector

Looking back to the survey responses for certification, education, and experience, the requirements for the IA/Security Engineer were really across the board. However, the majority of the responses provided were less than what you would expect for a position titled "Engineer". Again, using the criteria of an individual with at least a 4-year highly technical degree, heavily based on mathematics and whose skills and knowledge have been verified by a recognized governing and or licensing body to compare against. Although 74% required at least a bachelor's degree, 16% required none. Only 67% required an IA/security certification, 33% were not required or optional. The two most common certifications that were not reported in the survey responses but were found in many online job postings are the Cisco Certified Network Associate (CCNA) and the Microsoft Certified Systems Engineer (MCSE). The unique aspect here is that they are vendor certifications that have some security added in but are not pure security certifications.

When consolidating the technical requirements of online job postings for IA/Security Engineers, the skill set becomes very wide as one might expect. However, when an analysis of the knowledge/skills and related experience is performed, a different picture starts to develop. Skills and knowledge required included: (Dutcher, 2010)

- Fundamentals of network routing & switching
- Expertise in TCP/IP; web architectures and technologies such as HTML, JavaScript, XML, REST, PHP
- Web application penetration testing experience identifying architectural design weaknesses from analyzing a web application
- Implementing PKI components in a network, application and architecture and authentication capabilities of Windows, UNIX, Linux, Apple and middleware
- Experience with database technologies, architectural reviews and PCI-DSS.

Specific IA/Security related experience included Data-at-rest encryption, certificate validation, IDS/IPS, Firewalls, SEIMs and Log Management, syslog analysis, HTTP and TCP/IP

analysis, and vulnerability assessment to include; cross-site scripting, SQL injection, cross-site request forgery, HTTP response splintering, the OWASP Top 10 and SANS Top 25 (Dutcher, 2010). The more specific tools identified were WebInspect, Core, Paros, BURP, Cisco PIX, Checkpoint NG, Juniper & Netscreen Firewalls, Snort IDS, Tumbleweed, and Corestreet (Dutcher, 2010).

The analysis developed from this research is that the commercial/public sectors requirements demonstrate that organizations are really identifying IA/security experts of one type or another. The combination of some very specific technical requirements and expertise with tools and technologies but not a unanimous calling for formal education or certification essentially classifies these positions as administrators, technicians, operators, managers and analysts.

3.3.2. DoD Sector

Consistent with the IASAE job description, roles and functions outlined in DoD8570.01M, the minimum requirements for an individual to perform the duties of an IASAE are also outlined. The four primary categories are Experience, Knowledge, Other, and IA Certification. These are summarized below.

Experience: An IASAE level I is usually an entry level position requiring no IASAE experience. An IASAE Level II has at least 5 years of IASAE experience. The top end of the scale is the IASAE Level III with at least 10 years of IASAE experience (ASD(NII)/DoD CIO, 2010).

Knowledge: An IASAE Level I is required to be able to apply their knowledge of IA policy, procedures, and structure to design, develop, and implement computing environment system(s), system components, or system architectures. An IASAE Level II takes this a step further and is required to be able to apply their knowledge of IA policy, procedures, and workforce structure to design, develop, and implement a secure network environment. The Senior, IASAEA Level III must be able to apply their knowledge of IA policy, procedures, and workforce structure to design, develop, and implement a secure enclave environment . (ASD(NII)/DoD CIO, 2010)

Other: Local nationals (LNs) are authorized to perform duties as an IASAE Level I. However, LN opportunities are extremely limited and must meet requirements of DoD

Instruction 8500.2, Information Assurance (IA) Implementation. IASAE Level III positions are required to be filled by a U.S. Citizen (ASD(NII)/DoD CIO, 2010).

IA Certification: Within 6 months of assignment to position, CISSP, CISSP-ISSEP, CISSP-ISSAP (ASD(NII)/DoD CIO, 2010).

One may notice that even the DoD has issues with the IASAE Level I requiring no experience. However, the publication states that no IASAE experience is required, not that no IA or IT experience is required. Another criteria that the DoD is lacking are education requirements. There are currently no education requirements of any type identified in DoD 8570.01M for the IASAE. One could surmise that some form of education requirement is imposed through other directives and guidance but it was not evaluated in the scope of this paper.

Now, just as was documented prior about the draft update of DoD 8570.01M addressing shortfalls, they have in the requirements area as well. Currently in the draft, IASAEs will have system engineering (SE) and architecture requirements. A baseline is set at the lowest position and builds (in addition to, not in lieu of) through the progression. These new requirements are also applied to the IA Software Engineer position. Also under the draft proposal is a complete revamp of the required IA certifications and again changing throughout the progression of the positions (DoD 8570.01M Chapter 10 Rewrite Draft, 2010).

Although the DoD has gone to great lengths to improve their IA workforce and the IASAE position, there are still areas of concern. These concerns and their implications are addressed in the next section in combination with the commercial/public IA/Security Engineer.

3.4. Current Implications (Comparing to a PE)

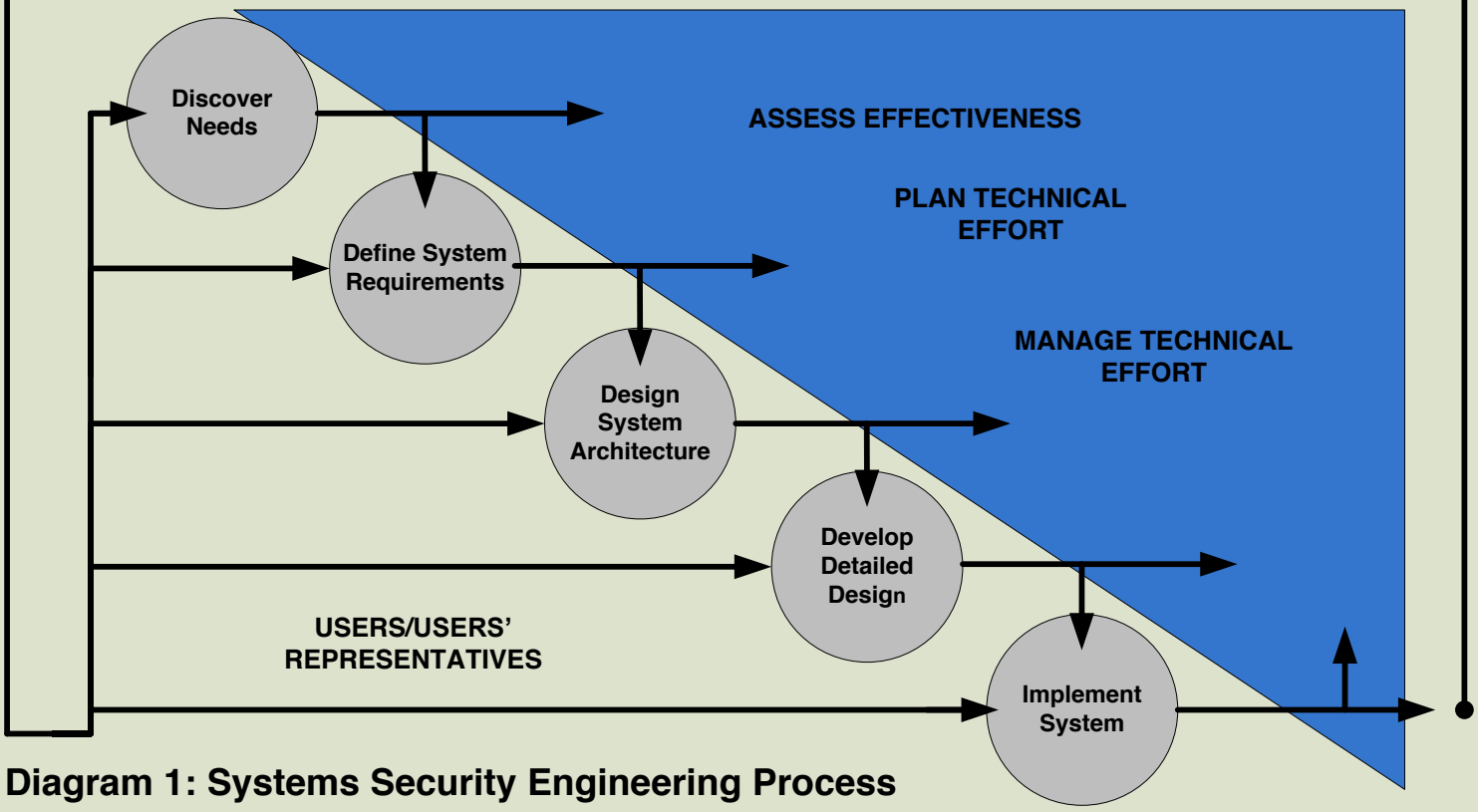

Diagram 1: Systems Security Engineering Process
(National Security Agency, Information Assurance Directorate, 2003)

The NSA may have provided the best definition of an IA Engineer when they worked with ISC^2 to develop the Information System Security Engineering Professional certification. Their exact definition is as follows [sic] "The art and science of discovering users security needs and designing and making, with economy and elegance, (information) systems so that they can safely resist the forces to which they may be subjected" (National Security Agency, Information Assurance Directorate, 2003). This is also depicted in the process flow NSA presents in Diagram 1 (National Security Agency, Information Assurance Directorate, 2003).

Professional Engineers (PEs) have always been a bit disgruntled with the IT industry in general and the haphazard use of the term engineer. When you take into account what it takes to achieve the licensed PE status, you'll start to understand why. PEs must complete a four-year engineering degree from an accredited university, pass the Fundamentals of Engineering (FE) exam, complete a four year apprenticeship under a PE, and then pass the Principles and Practice

of Engineering (PE) exam before becoming licensed (NSPE). This is a far cry from a Microsoft boot camp focused on passing the battery of Microsoft (only) technology exams or studying for the CISSP engineering focused ISSEP. Granted both are fine achievements, but do they really compare to the level of rigor required to be a PE? The Microsoft MCSE is single vendor focused but does consider architecture, design, implementations, and operations. The CISSP-ISSEP, the only IA Engineering labeled certification, is comprised of four domains (Systems Security Engineering, Certification and Accreditation, Technical Management, and U.S. Government Information Assurance Governance) that is heavily U.S. Government/DoD centered ((ISC)2). In addition, half of the Certification and Accreditation (C&A) domain is based on the DoD Information Technology Security Certification and Accreditation Process (DITSCAP) and DoD Instruction 5200.40, which were officially suspended and superseded in November 2007 by DoD Instruction 8510.01, DoD Information Assurance Certification and Accreditation Process (DIACAP) ((ISC)2), (ASD(NII)/DoD CIO, 2007). The final assessment is that IA, nor IT, have a comparable skill evaluation processes that equates to the level of specialized skill, knowledge, and competency as the licensed PE.

This assessment is emphasized when comparing the PE requirements to the IA/Security field's requirements. The following table lists some high level comparisons of these two vocations.

	Professional Engineer	IA/Security Engineer
4-Year degree required	Yes	No, completely dependent upon industry and organization
Apprenticeship required	Yes	No, completely dependent upon industry and organization
Certification required		No, completely dependent upon industry and organization
Licensure required	No, completely dependent upon industry, organization and role	No, none exists
Exam required	To be licensed yes, FE & PE	Only for certifications, single for most, ISSEP/ISSAP require the CISSP first. Most stringent and current IA pinnacle is the GIAC

		GSE (minimum 6 baseline & pre-requisite certifications)
Code of ethics	Yes, one common standard	Yes, multiple depending on certifying organization.
License legally required to prepare, sign, and submit engineering plans to a public authority or seal work for public & private clients	Yes	No
Bear the legal responsibility for their work and the lives affected by their work	Yes	No
License legally required for a consulting engineer or private practitioner	Yes	No

(NSPE), (GIAC Security Expert (GSE), 2009)

The result of IA/security technicians, administrators, analysts, etc being inappropriately labeled engineers is multifaceted. The most serious aspect in terms of a consultant is that their actual skills can be overestimated resulting in a false sense of security to the employing organization or the customer. Just because we place a default configured firewall at the network perimeter does not make us secure, neither does hiring an IA/Security "Engineer". Second, if an organization is paying for an IA/Security Engineer, it should receive for a cost benefit for it expenditures. Lastly is an idea the corporate counsels will have to debate. This paper is in no way providing legal advice; however, many are under the belief that if an organization is providing a service to the public, representing themselves as an engineer and they are indeed not, they could be held liable for falsely stating qualifications. Managers finding themselves in this type of scenario should at the very minimum consult their corporate legal counsel to investigate the matter as it pertains to their state laws.

4. Utilizing an IA/Security Engineer in the Organization

Now that a baseline understanding of what roles and responsibilities are assigned to a IA/Security Engineer, the next step is putting this knowledge into action. In order to reap the full benefits of an IA/Security Engineer, the manager must first take some steps to ensure success as failure is not an option. The full potential of the IA/Security position, the personnel and the organization could not be realized if we just stop here. There are further steps we can take to direct the development of the position throughout industry.

4.1. Resulting Benefits of an IA/Security Engineer (In-House Staff or Outsourced Contractor)

Organizations make changes for a purpose, to increase productivity, increase profit or save resources. You may ask how utilizing an IA/Security Engineer appropriately and efficiently equates to this. Well, it can and does on several fronts and these benefits can be realized through the use of in-house staff or outsourced to a contractor.

First and foremost, having the right personnel in the right position can make all the difference in the world. One aspect is that the organization can, and probably is overpaying personnel in "engineering" titled billets that are not really engineers, but really technicians and administrators. By using the term correctly and assigning personnel with the proper credentials to be called an IA/Security Engineer the organization has the opportunity to reap other benefits as well.

With a true IA/Security Engineer in the position, the organization has the opportunity to develop solutions that meet compulsory requirements, are secure the first time around and at a reduced cost. It is a common fact that IT projects are rarely on time or on budget. A 2009 CIO article states from a survey of 400 companies, only 32 percent of IT projects were successful, the criteria being on time and on budget. This left 24 percent as failed and 44 percent as challenged (Levinson, 2009). Now it would be absurd to assess that an IA/Security Engineer could have saved all these projects but it could have saved some. The ability to properly identify and document requirements from the start is a must for project success and the same is true for security requirements. This will ensure requirements are indentified from the beginning and built into the project throughout its lifecycle. Identifying security requirements at the beginning and ensuring they are worked also minimizes the risk of vulnerable systems being deployed which can expose the organization to unforeseen threats. Delivering projects on time and on

budget while not having to waste resources on the costly development of patching vulnerabilities will more than pay for having an experienced and qualified IA/Security Engineer on staff.

4.2. Standardizing the IA/Security Engineer definition/description

No industry or sector is spared in the misclassification and misuse of the term engineer. In this regard, even the DoD is not spared with the improper classification of the term engineer. DoD 8570.01M calls out tasks and functions for the IASAE that are operational in nature and should be grouped under the classification of IA Technicians (IATs). What has resulted is a modern day instance of what comes first, the chicken or the egg. As predicted, it depends who you ask. Some industry experts believe that organizations in all sectors follow the path paved by the certification bodies (ISC2, GIAC, ISACA, etc). Other believe that the federal government and DoD should pave the way as the largest single employer of IA/security professionals to force the certifications bodies to conform. However, this does not always work and the CISSP-ISSEP is the perfect example. The CISSP-ISSEP is an IA/security certification designed by the government, for the government. This alignment is not a good fit for the commercial/public sector due to the overwhelming differences in organizational structure, process and policy. This is especially true for smaller consulting firms providing services to small-medium business (SMBs) where levels of organization and technical complexity do not exist, but the need for secure and reliable solutions do.

Unfortunately there is no simple solution or "silver bullet" overnight success plan that can be implemented to correct the current situation. What the industry ultimately needs is a common agreed upon understanding of the IA/Security Engineer. This will provide the ability to determine an expected or minimum level of education, knowledge, experience, and skill required to be an IA/Security Engineer. This needs to be developed by a consensus and come from a consortium of certification providers, academia, government and industry. A lofty goal indeed but there are a few steps we as IA professionals and managers can take to make a concerted effort over time and the persistence to persuade the certification bodies and government organizations to change. The preferred way of change would be proactive measures taking positive steps forward by the consortium. The feared method of change will be one that is demanded and brought forth by governments resulting from fallout after a major cyber incident or disaster.

The first step, as IT and IA/Security managers, is to ensure our positions are properly classified and titled. A true technician or junior administrator with no engineering experience should not be assigned the positional title of engineer. Doing so degrades the title and position. As managers, we must do the right thing, make the hard decisions, and classify the positions correctly and appropriately.

Second, we need to work with and provide feedback to the certification bodies to create stringent engineering focused courses and certifications that test the true competency and use of skills. The IA/Security Engineer requires more than the ability to answer a battery of multiple choice questions.

The third step is for the certification bodies developing an engineering certification. This new IA/Security Engineering certification will need to demonstrate enough rigors to establish a new standard. An outcome that would not improve the situation is if the same group of administrators and technicians are certified as IA Engineers without adding rigor and raising the bar high enough. A challenge for the certification bodies will be ensuring the certification remains current and applicable. Developing a certification based on outdated technology and concepts would not provide the adequate level of assurance in the certification. Technology and threats are constantly adapting and emerging and so too must the certifications and those that are certified.

Lastly, as a profession and an industry we need to create a common set of ethical standards and an overarching body for all IA/security professionals. This will not only benefit the IA/Security Engineer, but all IA/security professionals.

5. Summary

This may be perceived as a complicated managerial policy problem, but it can be simplified quite effectively. This really comes down to classifying IA positions correctly and assigning the personnel with the proper credentials to the IA/Security Engineer position. By doing this, your organization will benefit from the proper implementation and usage of an IA/Security Engineer.

In comparison, if we have required licensed PEs in multiple other disciplines to design our critical infrastructure of roads, bridges, buildings, electrical power, water, and sewer; wouldn't we want IA/Security Engineers to have a similar rigor for designing, deploying and

implementing the protection of these critical systems? The next time you drive across a bridge that crosses a gorge think about this, would you want a licensed PE to have designed that bridge or someone who is good at multiple choice tests? You can use this same analogy the next time you fly in a plane or ride the Metro. You decide, a licensed PE or a boot camp crammer, and see how you feel. Using at all the developed commercial and custom applications, systems, and networks that have been designed and engineered with major flaws and vulnerabilities is a good example. There is a very high probability that they would not be nearly as vulnerable as they are today if they had been designed and implemented with this same level of rigor.

The licensing of professional engineers came about because of public safety concerns at the turn of the century. Many scholars use the analogy that the IT/IA industry and profession are in an equivalent stage of development, the end of the American Wild West. But what cyber tragedy will have to occur before the industry and government realizes that something must be done? Licensing of the profession does not present itself as the perfect solution to the current situation. Rather a more effective and efficient solution would be for organizations like SANS, ISC^2, ISACA and NIST to work with government, industry and academia in developing a standardized and recognized job description. This standardization would include position requirements and rigorous skills based certification process. Time will tell, but it is always better to be proactive and shape policy than to be reactive and be driven by it. As IA/Security and IT managers and leadership of all industries and sectors, government and civilian, we hold our future in our hands, lets shape the policy today.

Brian Dutcher, bdutcher.ia@gmail.com

6. References

(ISC)2. (n.d.). *(ISC)2 CISSP-ISSEP CBK Review Seminars*. Retrieved July 25, 2010, from (ISC)2: https://www.isc2.org/isseprevsem/default.aspx

(ISC)2. (n.d.). *Official (ISC)²® Guide to the CISSP-ISSEP® CBK®*. Retrieved Jul 25, 2010, from (ISC)2: http://www.isc2education.org/store/product_info.php?cPath=9&products_id=41

(ISC)2. (2010). (ISC)2 Company History: 20 Years of Excellence. Retrieved October 4, 2010, from (ISC)2: https://www.isc2.org/isc2-history.aspx

(2010, June). *DoD 8570.01M Chapter 10 Rewrite Draft* , 1-2. Washington D.C.: U.S. Deptartment of Defense.

ASD(NII)/DoD CIO. (2010, Apr 20). Department of Defense 8570.01M. *Information Assurance Workforce Improvemnet Program* , 16-20. Washington D.C.: Department of Defense.

ASD(NII)/DoD CIO. (2007, Nov 28). Department of Defense Instruction 8510.01. *DoD Information Assurance Certification and Accreditation Process (DIACAP)* , 1. Washington D.C.: U.S. Department of Defense.

Dutcher, B. (2010, Feb). An Information Assurance Workforce Evaluation of System-X: The Information Assurance Systems Architect and Engineer (IASAE). *Masters Thesis* , 18. Northfield, Vermont: Norwich University.

Carlson, B., Burgess, A., & Miller, C. (n.d.) Timeline of Computing History. Retrieved October 4, 2010 from, http://www.rci.rutgers.edu/~cfs/472_html/Intro/timeline.pdf

Federation of American Scientists. (2006, Feb 6). NSA/NCSC Rainbow Series. Retrieved October 4, 2010 from, http://www.fas.org/irp/nsa/rainbow.htm

GIAC Security Expert (GSE). (2009, Oct 12). Retrieved July 25, 2010, from Global Infromation Assurance Certification (GIAC): http://www.giac.org/certifications/gse.php

GIAC. (2010). GIAC InformationSecurity Certification - Program Overview. Retrieved October 4, 2010, from Global Infromation Assurance Certification (GIAC) http://www.giac.org/overview/

Levinson, M. (2009, Jun 18). *Recession Causes Rising IT Project Failure Rates*. Retrieved Aug 9, 2010, from CIO: http://www.cio.com/article/495306/Recession_Causes_Rising_IT_Project_Failure_Rates_

National Security Agency, Information Assurance Directorate. (2003, Dec 23). *Information Systems Security Engineering Professional (ISSEP).* Retrieved July 25, 2010, from www.acsac.org: http://www.acsac.org/2003/case/thu-c-1530-Oren.pdf

Naraine, R. (2004, Jun 29). U.S. CERT: Beware of IE. InternetNews.com - Security. Retrieved October 4, 2010, from http://www.internetnews.com/security/article.php/3374931/US-CERT-Beware-of-IE.

NSPE. (n.d.). *Licensure: What is a PE?* Retrieved July 26, 2010, from National Society of Professional Engineers (NSPE): http://www.nspe.org/Licensure/WhatisaPE/index.html

7. Appendix 1: DoD 8570.01M, IASAE Level I-III Functions

Table C10.T3. IASAE Level I Functions

IASAE-I.1. Identify information protection needs for CE system(s) and network(s).
IASAE-I.2. Define CE security requirements in accordance with applicable IA requirements (e.g., Reference (b), Director Central Intelligence Directive 6/3 (Reference (t)), organizational security policies).
IASAE-I.3. Provide system related input on IA security requirements to be included in statements of work and other appropriate procurement documents.
IASAE-I.4. Design security architectures for CE system(s) and network(s).
IASAE-I.5. Design and develop IA or IA-enabled products for use within a CE.
IASAE-I.6. Integrate and/or implement Cross Domain Solutions (CDS) for use within a CE.
IASAE-I.7. Design, develop, and implement security designs for new or existing CE system(s). Ensure that the design of hardware, operating systems, and software applications adequately address IA security requirements for the CE.
IASAE-I.8. Design, develop, and implement system security measures that provide confidentiality, integrity, availability, authentication, and non-repudiation.
IASAE-I.9. Develop and implement specific IA countermeasures for the CE.
IASAE-I.10. Develop interface specifications for CE system(s).
IASAE-I.11. Develop approaches to mitigate CE vulnerabilities, recommend changes to system or system components as needed
IASAE-I.12. Ensure that system designs support the incorporation of DoD-directed IA vulnerability solutions, e.g., IAVAs.
IASAE-I.13. Develop IA architectures and designs for DoD IS with basic integrity and availability requirements, to include MAC III systems as defined in References (b) and (f); systems with a Basic Level-of-Concern for availability or integrity in accordance with Reference (t); and other DAA designated systems.
IASAE-I.14. Develop IA architectures and designs for systems processing Sensitive Compartmented Information (SCI) that will operate at Protection Level 1 or 2 as defined in Reference (t).
IASAE-I.15. Assess threats to and vulnerabilities of CE system(s).
IASAE-I.16. Identify, assess, and recommend IA or IA-enabled products for use within a CE; ensure recommended products are in compliance with the DoD evaluation and validation requirements of References (b) and (f).
IASAE-I.17. Ensure that the implementation of security designs properly mitigate identified threats.
IASAE-I.18. Assess the effectiveness of information protection measures utilized by CE system(s).
IASAE-I.19. Ensure security deficiencies identified during security/certification testing have been mitigated, corrected, or a risk acceptance has been obtained by the appropriate DAA or authorized representative.
IASAE-I.20. Provide input to IA C&A process activities and related documentation (system lifecycle support plans, concept of operations, operational procedures and maintenance training materials, etc.).
IASAE-I.21. Participate in an IS risk assessment during the C&A process and design security countermeasures to mitigate identified risks.
IASAE-I.22. Provide engineering support to security/certification test and evaluation activities.
IASAE-I.23. Document system security design features and provide input to implementation plans and standard operating procedures.
IASAE-I.24. Recognize a possible security violation and take appropriate action to report the incident.
IASAE-I.25. Implement and/or integrate security measures for use in CE system(s) and ensure that system designs incorporate security configuration guidelines.
IASAE-I.26. Ensure the implementation of CE IA policies into system architectures.

Brian Dutcher, bdutcher.ia@gmail.com

IASAE-I.27. Obtain and maintain IA certification appropriate to position.

Table C10.T5. IASAE Level II Functions

IASAE-II.1. Identify information protection needs for the NE.
IASAE-II.2. Define NE security requirements in accordance with applicable IA requirements(e.g., References (b) and (t) and organizational security policies).
IASAE-II.3. Provide system related input on IA security requirements to be included in statements of work and other appropriate procurement documents.
IASAE-II.4. Design security architectures for use within the NE.
IASAE-II.5. Design and develop IA or IA-enabled products for use within a NE.
IASAE-II.6. Integrate and/or implement CDS for use within a CE or NE.
IASAE-II.7. Develop and implement security designs for new or existing network system(s). Ensure that the design of hardware, operating systems, and software applications adequately address IA security requirements for the NE.
IASAE-II.8. Design, develop, and implement network security measures that provide confidentiality, integrity, availability, authentication, and non-repudiation.
IASAE-II.9. Design, develop, and implement specific IA countermeasures for the NE.
IASAE-II.10. Develop interface specifications for the NE.
IASAE-II.11. Develop approaches to mitigate NE vulnerabilities and recommend changes to network or network system components as needed.
IASAE-II.12. Ensure that network system(s) designs support the incorporation of DoD-directed IA vulnerability solutions, e.g., IAVAs.
IASAE-II.13. Develop IA architectures and designs for DoD IS with medium integrity and availability requirements, to include MAC II systems as defined in References (b) and (f), systems with a medium Level-of-Concern for availability or integrity in accordance with Reference (t), and other DAA designated systems.
IASAE-II.14. Develop IA architectures and designs for systems processing SCI that will operate at Protection Level 1 or 2 as defined in Reference (t).
IASAE-II.15. Assess threats to and vulnerabilities of the NE.
IASAE-II.16. Identify, assess, and recommend IA or IA-enabled products for use within an NE; ensure recommended products are in compliance with the DoD evaluation and validation requirements of References (b) and (f).
IASAE-II.17. Ensure that the implementation of security designs properly mitigate identified threats.
IASAE-II.18. Assess the effectiveness of information protection measures used by the NE.
IASAE-II.19. Evaluate security architectures and designs and provide input as to the adequacy of security designs and architectures proposed or provided in response to requirements contained in acquisition documents.
IASAE-II.20. Ensure security deficiencies identified during security/certification testing have been mitigated, corrected, or a risk acceptance has been obtained by the appropriate DAA or authorized representative.
IASAE-II.21. Provide input to IA C&A process activities and related documentation (e.g., system life-cycle support plans, concept of operations, operational procedures, and maintenance training materials).
IASAE-II.22. Participate in an IS risk assessment during the C&A process and design security countermeasures to mitigate identified risks.
IASAE-II.23. Provide engineering support to security/certification test and evaluation activities.
IASAE-II.24. Document system security design features and provide input to implementation plans and standard operating procedures.
IASAE-II.25. Recognize a possible security violation and take appropriate action to report the incident.
IASAE-II.26. Implement and/or integrate security measures for use in network system(s) and ensure that system designs incorporate security configuration guidelines.
IASAE-II.27. Ensure the implementation of NE IA policies into system architectures.

Brian Dutcher, bdutcher.ia@gmail.com

IASAE-II.28. Ensure the implementation of subordinate CE IA policies is integrated into the NE system architecture.
IASAE-II.29. Obtain and maintain IA certification appropriate to position.

Table C10.T7. IASAE Level III Functions

IASAE-III.1. Identify information protection needs for the enclave environment.
IASAE-III.2. Define enclave security requirements in accordance with applicable IA policies(e.g., References (b) and (t) and organizational security policies).
IASAE-III.3. Provide input on IA security requirements to be included in statements of work and other appropriate procurement documents.
IASAE-III.4. Support Program Managers responsible for the acquisition of DoD IS to ensure IA architecture and systems engineering requirements are properly addressed throughout the acquisition life-cycle.
IASAE-III.5. Design security architectures for use within the enclave environment.
IASAE-III.6. Design and develop IA or IA-enabled products for use within the enclave.
IASAE-III.7. Design and develop CDS for use within CE, NE, or enclave environments.
IASAE-III.8. Develop and implement security designs for new or existing enclave system(s). Ensure that the design of hardware, operating systems, and software applications adequately address IA security requirements for the enclave.
IASAE-III.9. Design, develop, and implement security measures that provide confidentiality, integrity, availability, authentication, and non-repudiation for the enclave environment.
IASAE-III.10. Design, develop, and implement specific IA countermeasures for the enclave.
IASAE-III.11. Develop interface specifications for use within the enclave environment.
IASAE-III.12. Develop approaches to mitigate enclave vulnerabilities and recommend changes to system or system components as needed.
IASAE-III.13. Ensure that enclave system(s) and network(s) designs support the incorporation
of DoD-directed IA vulnerability solutions, e.g., IAVAs.
IASAE-III.14. Develop IA architectures and designs for DoD IS with high integrity and availability requirements, to include MAC I systems as defined in References (b) and (f), systems with a high Level-of-Concern for availability or integrity in accordance with Reference (t), and other DAA designated systems.
IASAE-III.15. Develop IA architectures and designs for systems and networks with multilevel security requirements or requirements for the processing of multiple classification levels of data (e.g., UNCLASSIFIED, SECRET, and TOP SECRET).
IASAE-III.16. Develop IA architectures and designs for systems processing SCI that will operate at Protection Level 3, 4, or 5 as defined in Reference (t).
IASAE-III.17. Develop IA architectures and designs for DoD IS to include automated IS applications, enclaves (which include networks), and special purpose environments with platform IT interconnectivity, e.g., weapons systems, sensors, medical technologies, or distribution systems.
IASAE-III.18. Ensure that acquired or developed system(s) and network(s) employ Information Systems Security Engineering and are consistent with DoD Component level IA architecture.
IASAE-III.19. Assess threats to and vulnerabilities of the enclave.
IASAE-III.20. Identify, assess, and recommend IA or IA-enabled products for use within an enclave and ensure recommended products are in compliance with the DoD evaluation and validation requirements of References (b) and (f).
IASAE-III.21. Ensure that the implementation of security designs properly mitigate identified threats.
IASAE-III.22. Assess the effectiveness of information protection measures utilized by the enclave.
IASAE-III.23. Evaluate security architectures and designs and provide input as to the adequacy of security designs and architectures proposed or provided in response to requirements contained in acquisition documents.

Brian Dutcher, bdutcher.ia@gmail.com

IASAE-III.24. Ensure security deficiencies identified during security/certification testing have been mitigated, corrected, or a risk acceptance has been obtained by the appropriate DAA or authorized representative.
IASAE-III.25. Provide input to IA C&A process activities and related documentation (e.g., system life-cycle support plans, concept of operations, operational procedures, and maintenance training materials).
IASAE-III.26. Participate in an IS risk assessment during the C&A process and design security countermeasures to mitigate identified risks.
IASAE-III.27. Provide engineering support to security/certification test and evaluation activities.
IASAE-III.28. Document system security design features and provide input to implementation plans and standard operating procedures.
IASAE-III.29. Recognize a possible security violation and take appropriate action to report the incident.
IASAE-III.30. Implement and/or integrate security measures for use in the enclave and ensure that enclave designs incorporate security configuration guidelines.
IASAE-III.31. Ensure the implementation of enclave IA policies into system architectures.
IASAE-III.32. Ensure the implementation of subordinate CE and NE IA policies are integrated into the enclave system architecture.
IASAE-III.33. Oversee and provide technical guidance to IASAE Level I and II personnel.
IASAE-III.34. Obtain and maintain IA certification appropriate to position.

Last Updated: December 1st, 2020

Upcoming SANS Training

Click here to view a list of all SANS Courses

SANS Essentials Australia 2021	**Melbourne, AU**	**Feb 15, 2021 - Feb 20, 2021**	**Live Event**
SANS OnDemand	**OnlineUS**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**