Taking the Mystery out of Information Assurance for the 21st Century Training Community

William Kaczor
MTS Technologies
Orlando, FL
Kaczorw@mtstech.com

Craig Thornley
PEO STRI
Orlando, FL
Craig.Thornley@us.army.mil

Buddy Guynn
NAVAIR, Orlando
Orlando, FL
Buddy.Guynn@navy.com

ABSTRACT

Information Assurance (IA) is one of the most overlooked yet critical aspects of any Information Technology (IT) system. Although IA applies to every IT system, we will focus on its application to simulators and any IT powered training device connecting to a DoD network. IA is the overarching process consisting of Computer/Network/Data/Information Security. If IA is built into every training and education system, and maintained throughout its life cycle, it is guaranteed to lower compromising threats to DoD assets.

This paper will take the mystery out of IA, system security engineering, and the security Certification and Accreditation (C&A) process from both government and industry perspectives. It will provide proven solutions to achieve C&A on any system under differing conditions and time frames, and document the process of IA using proven systems security engineering processes, the DoD Information Technology Security Certification and Accreditation Process (DITSCAP), and the documentation strategy of using the System Security Authorization Agreement (SSAA) and the System Security Plan (SSP). This paper will also provide examples of Information Assurance Vulnerability Alerts (IAVAs), including how they work and greatly reduce the risk to all IT systems. It will present the best practices for new systems, blended certification approaches, how to certify legacy systems, and the proper end of life disposal.

The 21st century force is moving more toward a net-centric, real time, and IT-based integrated operational and training environment. To achieve war-fighting excellence, IA of computer systems and networks should be a major focus of all new system designs for protection of national defense information and assets.

ABOUT THE AUTHORS

William Kaczor is the IA Team Lead for MTS Technologies, Inc in Orlando, Florida. He has a degree in Information Technologies with a specialty in Networks and Network Security, and has multiple security certifications including Information Assurance Security Officer from the U.S Army and Cisco Certified Network Administrator. He has certified and accredited over 20 training and operational systems for all four branches of the DoD, and is currently the Lead Security Engineer for the US 101 Presidential Helicopter.

Craig Thornley serves as the Information Assurance Program Manager (IAPM) for the Program Executive Office for Simulation, Training and Instrumentation (PEO STRI). Craig is responsible for the IA of a $1.6 billion a year organization with over 1025 military, civilian, and industry personnel servicing over 334,000 training systems around the world. He holds a Bachelors of Science in Electrical Engineering (BSEE) from the University of Central Florida and has specialized training in security engineering and IA. Craig has 18 years of service to the Government focusing on military intelligence and IA.

Buddy Guynn serves as the Security Manager and Supervisory Security Specialist for NAVAIR Orlando Security Department Code 7.4 and serves as the lead for NAVAIR Orlando's System Security Engineering (SSE) initiative. He completed 20 years of service with the US Air Force Security Police, integrating defensive measures through program protection planning. When working for the Defense Information Systems Agency, he helped develop the current DoD IA C&A process. His specialized training includes: Security for Special Programs, DoD Security Institute, Information Based Warfare, National Defense University and Computer Security Officer Certification, and US Army Management Engineering College.

Taking the Mystery out of Information Assurance for the 21st Century Training Community

William Kaczor
MTS Technologies
Orlando, FL
Kaczorw@mtstech.com

Craig Thornley
PEO STRI
Orlando, FL
Craig.Thornley@us.army.mil

Buddy Guynn
NAVAIR, Orlando
Orlando, FL
Buddy.Guynn@navy.com

INFORMATION ASSURANCE: WHAT IS IT?

Information Assurance (IA) is a requirement assigned to all DoD Information Systems (IS) several dozen pages into a statement of work. IA is a requirement that DoD organizations have to fill, but it is often overlooked during development and budgeted incorrectly. This issue translates into a failure to incorporate security early-on in the system's design. When a design change is required at the end of development from improper security engineering up-front, it costs much more than if it was incorporated from the beginning. IA should be a major concern for all persons involved as war fighting becomes more computer and network centric. The complexities of IS today constantly require revamping security measures against the constant barrage of security threats.

This paper will demonstrate what IA is, how it can be used effectively, what some of the misconceptions of IA and IT security are, and the future of IA. This paper will also present an overview of the DoD Certification and Accreditation (C&A) process and propose a two-pronged approach at solving the continuing battle of security versus funding versus schedule.

IA, as defined in Army Regulation 25-2, is the "protection of systems and information in storage, processing, or transit from unauthorized access or modification; denial of service to unauthorized users; or the provision of service to authorized users. It also includes those measures necessary to detect, document, and counter such threats." IA is also the encompassing security protection umbrella that includes COMSEC, INFOSEC, COMPUSEC, PERSEC, Physical Security and TEMPEST.

The true definition of IA that this paper would like to illustrate is that IA is the umbrella of all system security measures and protections. If there is a task that involves protecting a training system, then IA needs to be implemented within the system development at the earliest possible stage. If IA is included within the acquisition or proposal phase of the program, then the probability for a successful and secure trainer to be fielded is greatly increased.

Within the IA structure there is a very detailed and defined procedure known as the DoD Information Technology Security Certification and Accreditation Process, also known as the DITSCAP. The DITSCAP requires a thorough security definition of the IT system, a validation of the security measures installed, and a verification of the security measures by an independent reviewer and final C&A maintenance. The document that contains the security information is the System Security Authorization Agreement, also known as the SSAA.

The SSAA is *the* document that lists the entire technological description of a system, its security concept of operations, all of the security requirements, and the policies that a system will follow. Within this document there will be a description of the who, what, when, where, and how a system is protected. The SSAA also contains security test plans and test procedures, security training plans, memorandum of agreements or understanding, involving special exceptions and cross boundary connections, as well as contingency plans, test results, life cycle management and configuration management policies.

The SSAA will also include, in a protected appendix, documentation of the system's vulnerabilities, the residual risk, and a mitigation strategy on how the contractor and the government can maintain security as threats evolve. The SSAA is a living document and needs to be continually updated. If the system changes, requirements increase, or new threats emerge, the SSAA needs to be updated to define, validate, and verify that the system can protect DoD data.

The IA Control requirements for a system are captured in the SSAA Appendix F, Security Requirements Tracability Matrix. There is a comprehensive list of upper level requirements in DoDI 8500.2. The requirements in 8500.2, and the service level regulations, can be linked to system level requirements of the program and can be traced all the way down to the component level. This flexibility allows the DITSCAP to be incorporated throughout the system design life cycle.

There are other forms of C&A programs that are documented in DCID 6/3 or JAFAN 6-3 that are used for more specialized programs. For the purposes of this paper, only DITSCAP, the applicable DoD 8500 series regulations, and applicable service regulations, will be discussed.

THE KEY MEMBERS OF THE DITSCAP

The following information regarding the key members of the DITSCAP are taken directly from DoD 8510.1-M. There truly is no better description than what this guidance provides. Each service also has slightly different names and roles for the key members that are documented in applicable service regulations.

Designated Approving Authority (DAA)

The DAA is the primary Government official responsible for system security. The DAA is the official responsible for accepting a level of risk for the operation of the training system. Based on national, agency, organizational policies and guidance, and input from the user representative and program manager, the DAA directs the security activities of the certifier.

The DAA is usually a senior operational commander with the authority and ability to evaluate the mission, business case, and budgetary needs for the system in view of the security risks. The DAA must have the authority to oversee the budget and IS operations of systems under his/her purview. The DAA determines the acceptable level of residual risk and approves the system operation. From experience, the DAA is usually a General Officer, Member of the Senior Executive Service in the Army, or a Captain or above in the Navy.

Program Manager

The program manager represents the interests of the system throughout its life cycle (acquisition or maintenance, life-cycle schedules, funding responsibilities, system operations, performance, and maintenance). The organization the program manager represents is determined by the phase in the life cycle of the system.

Certifier

The certifier (and certification team) provides the technical expertise to conduct the certification through the system's life cycle based on the security requirements documented in the SSAA. The certifier determines the level of residual risk and makes an accreditation recommendation to the DAA. The certifier also directs all vulnerability testing and mitigation plans.

User Representative

The operational interests of the systems users are vested in the user representative. In the DITSCAP process, the user representative is concerned with system availability, access, integrity, functionality, and performance in addition to confidentiality as they relate to the system mission.

The diagram below is an example of the C&A effort.

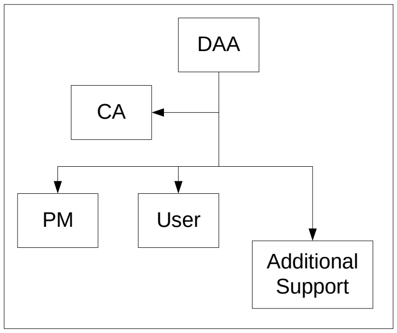

Figure 1. Members of the IA Process

THE FOUR PHASES OF THE DITSCAP

There are four phases to the DITSCAP: Definition, Verification, Validation, and Post-Accreditation. Each phase has a distinct and different goal. The intent of the process is to ensure and protect the DoD's IT systems from compromise. The goal is to create, field, and support a secure and usable system to train our military at a reasonable level of cost and at an acceptable level of security risk. Figure 2 below shows the four phases of the DITSCAP:

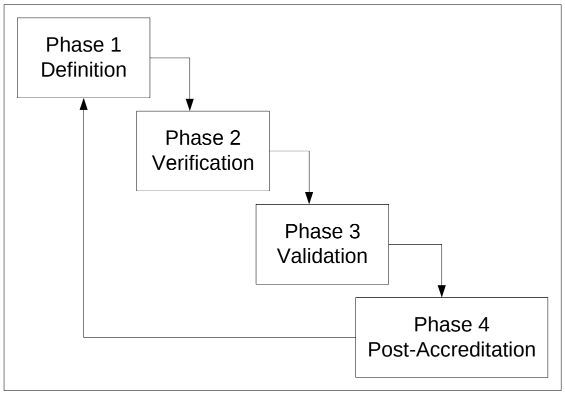

Figure 2. DITSCAP/SSAA Phases

DITSCAP Phase 1

Phase 1 defines the system and the applicable security requirements, and identifies the controlled interfaces. It begins the Security Concept of Operations so that users can learn how the system will be ultimately used. Phase 1 must be completed by the system's Design Readiness Review/Critical Design Review. Figure 3 illustrates the flow of Phase 1 activities.

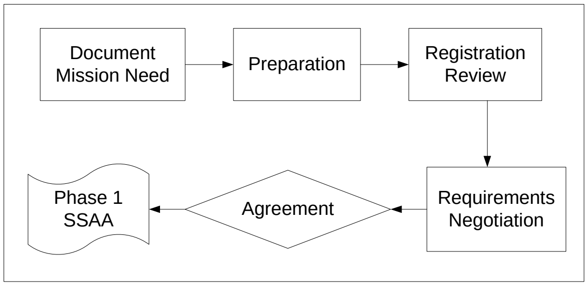

Figure 3. Phase 1 Activities

DITSCAP Phase 2

Phase 2 verifies that all of the requirements are being met, and the system design meets the government requirements. In this phase, test plans and procedures are written, internal testing is conducted, analysis reports identifying the vulnerabilities are composed, and residual risk including how that risk will be mitigated is documented. Phase 2 activities start from the approval of Phase 1 and are primarily conducted by the contractor with government direction. The activities for Phase 2 are listed in Figure 4.

During Phase 2, vulnerability and compliance scanning tools are used to determine where the shortfalls of the system design can be. Each service uses different tools, but the Defense Information Security Agency issues a "Gold Disk" that can be used to properly update a systems security profile.

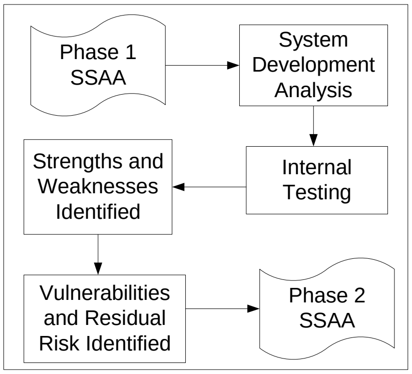
Phase 1 SSAA
System Development Analysis
Internal Testing
Strengths and Weaknesses Identified
Vulnerabilities and Residual Risk Identified
Phase 2 SSAA

Figure 4. Phase 2 Activities

DITSCAP Phase 3

In Phase 3 the official vulnerability testing is conducted by the government certifying agents. After the testing phase, there is a determination by the approving authority as to whether or not the system contains an acceptable level of risk to operate. If the risk is too high, from a new security threat or faulty design, then negotiations are held to best mitigate the issue. The entire flow of this process is illustrated in Figure 5. The system can be granted the following three types of clearance to operate:

- **Authority to Operate, ATO:** This type is full clearance to operate. The ATO is valid as long as the system remains in compliance with the SSAA, DITSCAP, and service requirements. The ATO is valid for three years unless there is a major system change requiring a new C&A effort.
- **Interim Approval to Operate, (IATO):** This clearance to operate is only given to mission critical systems. The IATO gives the time for any high risks to be mitigated but allows for training to commence due to operational requirements. The IATO is usually not longer then six months.
- **Interim Approval to Test (IATT):** This allows for the system to operate but only under specific conditions and a very limited time frame. An IATT is typically only valid for testing events and usually not for longer than 30 days. The system can be scanned/inspected by the approving authority to verify that it is being used in accordance with the IATT agreement.

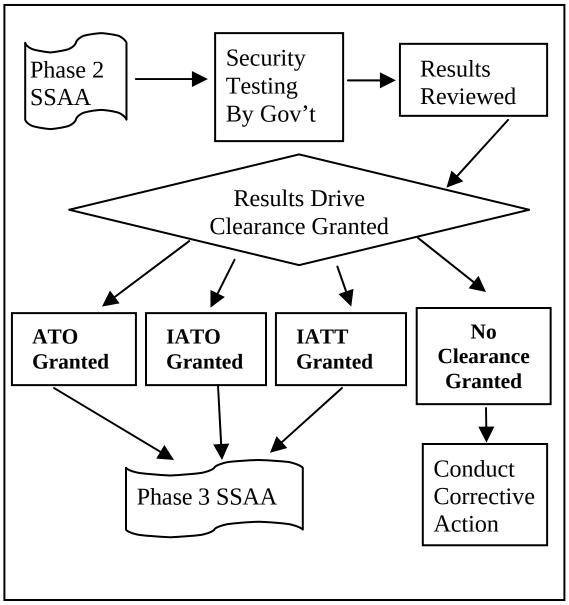

Figure 5. Phase 3 Activities

DITSCAP Phase 4

Phase 4, the Post-Accreditation phase, allows for the user community, contractor, and other government agencies to maintain security as the threats change. This is usually achieved by having an Information Assurance Vulnerability (IAVM) Plan. This plan describes to the user and contractor how security updates, patches, and policies should be updated throughout the life cycle management of the system.

The IAVM plan explains how the system will test and implement issued Information Assurance Vulnerability Alerts (IAVAs). IAVAs are issued through a national Computer Emergency Response Team (CERT). Each service has its own CERT to ensure that service requirements are met via the IAVA issuance.

Figure 6 lists a generic IAVM plan. IAVM plans can be tailored to operational needs and system designs but approval from deviations is provided by the DAA.

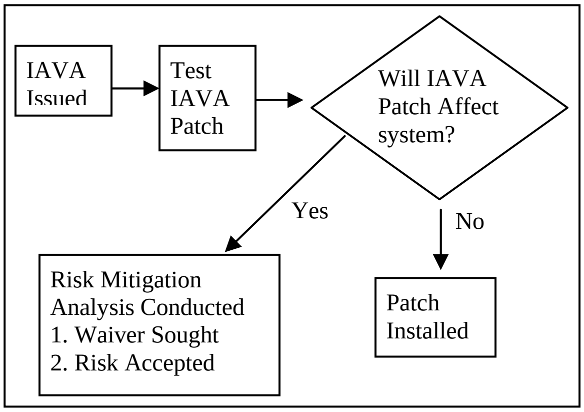

Figure 6. Phase 4 Activities

THE DITSCAP AND TRAINING SYSTEMS?

The Army and Navy have multiple paths that they can take as far as C&A efforts are concerned. The DITSCAP allows for a tailor-made process to fit the needs of schedule and cost while always assuring that the system is secure. The types of systems to be certified will directly dictate the effort in which both the command and the contractor certify and accredit a training system.

Types of IT Systems

IT systems can be divided into three general categories: classified non-stand alone, unclassified non-stand alone, and classified\unclassified stand alone devices. There are variants to each of these types, and if a unique issue arises, the flexibility of the DITSCAP will once again assure that the proper protection is in place.

Classified Non-Stand Alone Systems

A classified non-stand alone system is also known as a classified networked system. These are best defined as classified systems that connect to approved external networks. The best example of this can be a simulator that connects to another simulator via a secured connection. This can be accomplished using an NSA approved encryptor as well as implementing defined security protections that will be documented in the SSAA. This type of system is the most difficult to certify because it involves classified data that is being used and transmitted over the Internet. Although protected by encryption, there is significant risk associated to this process.

With a networked system, there is also the increase of effort with ensuring the network devices, servers, and workstations meet DoD/DISA Security Technical Implementation Guide (STIG) standards. This can be accomplished by manually following the STIG's or using a tool such as the DISA Gold Disk. There are additional DoD approved scanning tools to find the vulnerabilities and then test/patch the system in accordance with the systems IAVM Plan.

Unclassified Non-Stand Alone Systems

An unclassified non-stand alone system usually refers to a more familiar network training system. These systems are best defined as systems that connect to approved external networks, including computer-based maintenance training networks or even connected networks that support training devices.

The DITSCAP is designed to secure networks and this type of training system C&A usually is conducted much faster and is less expensive than a classified DITSCAP C&A effort.

Stand Alone Systems

A stand-alone system consists of a computer in a training room that does not hook up to any outside source. Each service has unique set of requirements for stand alone training systems. The best approach for a system like this is to complete a security baseline and update IAVA patches as necessary.

With the future constantly striving to network and integrate all training systems and devices, it is prudent to complete the DITSCAP process up to Phase 3. The reason for this is that it will save time and money if the system is required to be networked. Phase 2, as discussed earlier, allows for program managers to know where the vulnerabilities exist and as time and budget become available, the preparations to fix these issues should be addressed.

Types of Accreditation

There are two types of accreditation for DoD systems; site accreditations and type accreditations. Each of these accreditation types has different goals and processes in which to achieve ATO status.

Type Accreditations

A type accreditation is simply defined as an accreditation for a series of exact duplicate training devices. If an organization was to field ten networked desktop computers at a training facility that would teach military personnel how to complete a certain type of training, then a type accreditation could be used. A type accreditation gives flexibility to both the contractor and the government to build and ship devices that are fully accredited with security built in.

One concern of a type accreditation is that when a training system is fielded, a site accreditation must be accomplished for the system to connect to other training networks. This additional requirement can be easily managed as explained in the next section.

Site Accreditations

A site accreditation contains all site-specific security and protection methods and all the same information of a type accreditation. So the usage and protection of a training device is documented as well as the facility protection features. A site accreditation also includes documentation of access policies, protection methods for classified or sensitive data, and physical security measures commensurate with the site classification.

External Threats

There are constant threats to DoD systems from hackers and enemies of the country. On a daily basis, US STRATCOM is attacked an average of 150 times. This is an astronomical number based on the fact that it is one command within DoD.

Simulators are connecting more frequently to operational environments which will require more stringent security practices to be applied. The argument has been that training systems do not require tight security, have a lower threat, and have a small amount of information that can be compromised. Due to the added security concerns, this argument needs to end.

In a recent article from Space Command, Air Force Gen. Ralph E. Eberhart, U.S. Space Command Commander in Chief said, "my view is that as we look at our computer systems, we'd be kidding ourselves if we thought they weren't vulnerable." This quote is based on an internal evaluation of space commands operational and training networks.

The best external threat scenario is if a country unfriendly to our interests hacks into a training network that uses real weapons data, then the enemy can adjust their tactics in real war operations. If an enemy knows a rocket or air to ground missile specifications, they know where to place their units.

If training networks are given the same security considerations as operational networks, then there is one less piece of information that can be used against US troops.

Internal Threats

Recent espionage has shown that even though a person with a high security clearance is trusted, the information and computer networks can be compromised. “The Story of Aldrich Ames” is a classic example of how lax security causes internal threats to be more dangerous than external threats. Ames bypassed multiple levels of security and accessed computer files to gain information that was used against CIA covert operations. This clearly demonstrates the need to have a constant security plan and concept of operations in place to protect against even the unlikely scenarios.

IA IMPLEMENTATION STRATEGIES

The two implementation strategies that are used to secure training systems are: the “Baked In” and “Bolted On” security approaches. Security is perhaps one of the most important aspects of the DoD information and computer networks. These two approaches allow for different time lines to ensure that proper security protections are in place.

“Baked In” Security

“Baked In” security is best defined as the process that incorporates IA engineering and personnel right into the design and engineering phase of the system. In other words, IA is not above or below an Integrated Product Team, it is part of the process and team. This approach has the following major advantages:

- Full visibility of security requirements to the product engineering team
- The ability to build security directly into the solution with little disruption to schedule
- Security that goes right along with the change

process if system requirements change
- Lower cost when the initial Phase 1 process occurs and there can be a "lull" while the product is built
- Security testing alongside delivery efforts, conducted by the IA team when testing starts
- Assurance for program managers that security is not a concern during formal acceptance testing when the product is delivered
- Government and contractor program mangers will know if there is residual risk, exactly what is at risk, and have a mitigation strategy in place
- SSAA will be built as the system is, therefore, a full definition of the system, from a security aspect, will be written alongside other system documents

In summary of the "Baked In" approach, security is built into the system as it is being developed. The cost of security is spread out over the schedule more effectively, and the schedule is easier to meet because the IA C&A efforts make sure there are no surprises. This implementation strategy provides the most security, at the least risk to system use, and is the preferred method of IA implementation.

"Bolted On" Security

The "Bolted On" approach is designed for already fielded systems, legacy systems, or systems that are about to be fielded that do not have any C&A documentation. This situation is prevalent in many legacy systems and in a lot of contracts that were written without an IA requirement. The highlights of this process include:
- IA engineers that are forced to match requirements with an existing design
- Little room for change to the system design as the system is usually fielded
- Increase in testing as the system was designed one way, and the requirements may push the system to do something that it was not designed to do
- Considerable amount of waivers to be expected and many grey areas to traverse
- Increased cost due to the schedule requiring certification in a short time period (usually ASAP)

CLEARING UP IA CONCERNS

During the DITSCAP process, there are constant questions regarding cost, schedule, levels of protection, and the plan for emerging threats.

Cost

The question of cost is constantly asked during a proposal phase and even during the actual work. Questions arise such as "what are we getting for this?" A simple sanity check is to examine the systems classification level, its mission, and the schedule. From these three items, a decision must be made on how the IA team should be constructed.

An additional question that needs to be answered is what is the MAC, or Mission Assurance Category, Level? The MAC Level is determined by the weighting of the system security requirements. There are three MAC Levels, and they assist in determining the set of requirements that the IA Team needs to follow during the C&A effort.

Cost is primarily determined by the level of effort associated with the MAC and Confidentiality level.
The MAC level, as defined in DoDI 8500.2, reflects the importance of information relative to the achievement of DoD goals and objectives, particularly the warfighters' combat mission.

The higher the classification, the more security requirements result. The more security requirements, the more validation and verification required to meet those requirements, hence the larger the IA effort. The majority of trainers are at a lower classification level due to the operational necessity level.

The system security characteristics and weight will determine which certification tasks, according to DoD 8510.1 -M, required to be accomplished. Tables 1 and 2 below demonstrate the weighting process for a standard classified non-stand alone trainer and a description of the certification level of tasks that need to be accomplished. Table 1 is the detailed information of a training system that is needed to determine the Certification Level that is illustrated in Table 2.

Cost vs. Protection

Within IA there is always a cost vs. protection battle. The level of acceptable risk is completely left up to the DAA with support from the CA, Contractor PM, and the User Representative. The decision regarding the level of acceptable risk for any system is determined by the DAA with the rest of the IA team's input and recommendation.

Schedule

An additional piece to the acquisition strategy is schedule. There are usually many questions about when certain C&A Milestones must be accomplished in conjunction with the acquisition and fielding milestones.

Table 1. IA Characteristics and Weighting

Characteristic	Alternatives and Weights	Weight
Interfacing Mode	Benign (w=0), Passive (w=2), Active (w=6)	**6**
Processing Mode	Dedicated (w=1), System High (w=2), Compartmented (w=5), Multilevel (w=8)	**2**
Attribution Mode	None (w=0), Rudimentary (w=1), Selected (w=3), Comprehensive (w=6)	**3**
Mission-Reliance	None (w=0), Cursory (w=1), Partial (w=3), Total (w=7)	**1**
Availability	Reasonable (w=1), Soon (w=2), ASAP (w=4), Immediate (w=7)	**2**
Integrity	Not-applicable (w=0), Approximate (w=3), Exact (w=6)	**6**
Information Categories	Unclassified (w=1), Sensitive (w=2), Confidential (w=3), Secret (w=5), Top Secret (w=6), Compartmented/Special Access Classified (w=8)	**3**
	Total weights	**23**

Table 2. IA Certification Level

Level	Calculation	Certification Level	Description
1	If the total of the weighting factors is < 16.	Minimum Security Checklist	Level 1 requires completion of the minimum-security checklist. The system user or an independent certifier may complete the checklist.
2	If the total of the weighting factors is 12-32.	Minimum Analysis	Level 2 requires completion of the minimum-security checklist and independent certification analysis as defined in the Verification and Validation phases.
3	If the total of the weighting factors is 24-44.	Detailed Analysis	Level 3 requires completion of the minimal security checklist and more in-depth, independent analysis as defined in the Verification and Validation phases.
4	If the total of the weighting factors is 38-50.	Extensive Analysis	Level 4 requires completion of the minimal security checklist and the most extensive independent analysis as defined in the Verification and Validation phases.

Figure 7 displays the schedule used by PEO STRI for acquisition of new devices. In this schedule, both government and contractor development teams can see that the process starts six months before the actual development of a trainer and is completed within 24 months (for a typical two-year program). The time frame can be lengthened or condensed as per system fielding schedule as well as budget concerns.

The compression of a schedule will always affect the thoroughness of a security evaluation and could cause for security vulnerabilities to be missed. The opposite argument, that a system can take too long to certify and accredit, should also be a concern. Too long of a schedule is an issue because technology is always growing and legacy devices are more susceptible to attacks due to manufacturers no longer supporting security patch issuance.

CONCLUSION

The future holds greater ease of use for the IA process. The Defense Information Assurance Certification and Accreditation Process (DIACAP) is a more automated process with much more visibility. The security in this automated process will be dictated and patches, updates, and upgrades will become more frequent and impossible to avoid.

The future will also bring many more capable security engineers. DoD 8570 mandates that contractors shall

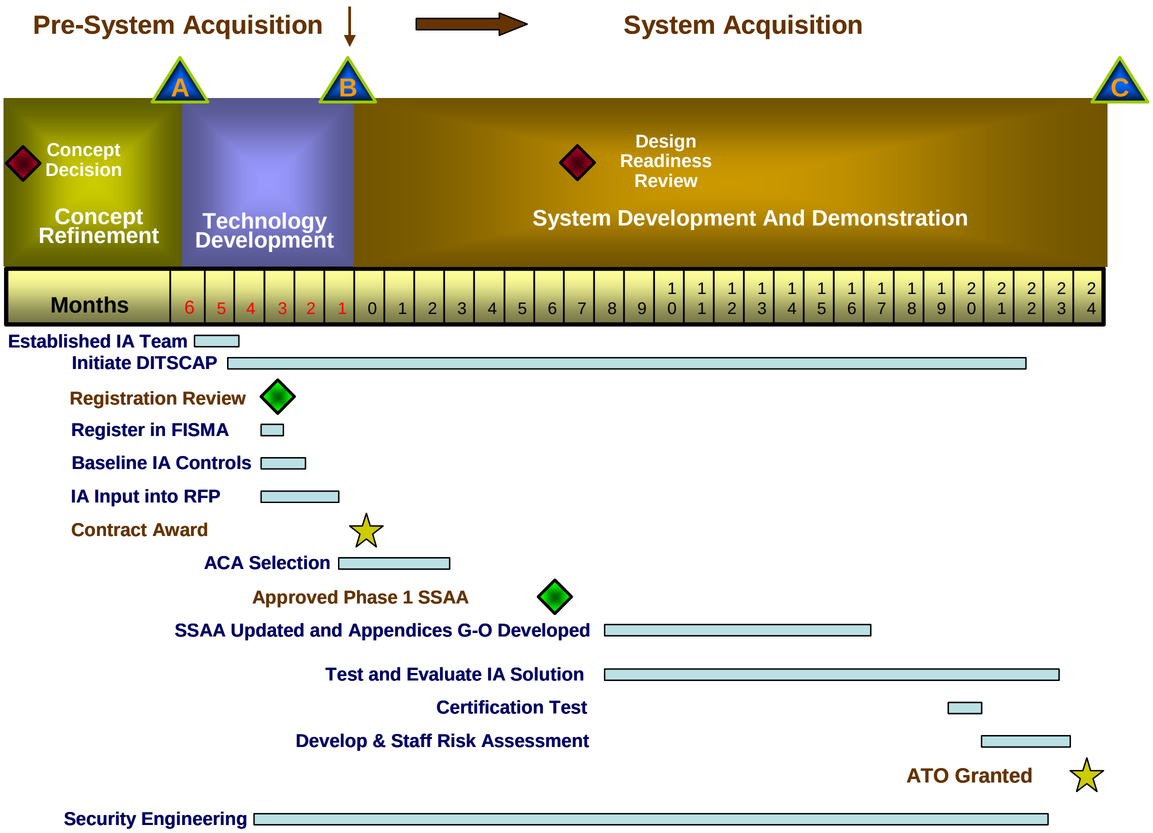

Figure 7. PEO STRI IA Milestone Schedule

have Certified Information System Security Professionals (CISSP) or other security certified professionals on staff. The mandates in DoD 8570 will enhance the capability of the IA Teams with dedicated engineers who are solely specialized in IT Security.

IA should be the main focus of all new training devices for a multitude of reasons. Most of these reasons are listed in this paper. The main focus is that IA is needed, and it should not be burdensome. It should enhance the training environment.

IA should be viewed upon as a protector, not a road block. IA can enhance the next generation of trainers. Also, the entire DoD IT infrastructure can be used without fear of attack or denial of service. Contractors that incorporate IA during their development cycle will be able to feel at ease knowing that they are delivering a secure and ready to use system to the DoD. When IA is incorporated from the start, it can make the difference of how our troops train in the 21st century.

REFERENCES

Department of the Army, Army Regulation 25-2. (2003). *Information Assurance*.

Department of Defense, 8510.1-M. (2000). *DITSCAP Application Manual*.

Department of Defense Directive, 8500.1. (2002). *Information Assurance*.

Department of Defense Instruction, 8500.2. (2003). *Information Assurance Implementation*.

Department of the Navy, 5239. (2005). *Information Assurance Program*.

Earley, Pete. (2005). CIA Traitor Aldrich Ames. *CourtTV Crime Library*. Retrieved June 6, 2006, from http://www.crimelibrary.com/terrorists_spies/spies/ames/1.html.

Gilmore, Gerry. (2001). Computer Security Threat Is Real, SPACECOM Chief Says. *American Forces Information Service*. Retrieved May 31, 2006, from http://www.defenselink.mil/news/Apr2001/n04052001_200104053.html.

Hebert, Adam. (2005). Information Battleground. *Air Force Magazine*. Retrieved May 13, 2006, from http://www.afa.org/magazine/Dec2005/1205info.html,