Implementing Information Assurance – Beyond Process

Misty Piatek
Booz Allen Hamilton
Johnstown, PA
Piatek_Misty@bah.com

James Newkirk
PEO STRI
Orlando, FL
James.R.Newkirk@us.army.mil

ABSTRACT

Information Assurance (IA) has been around for decades and has finally obtained the attention it deserves. Ten years ago, the term "IA" was known only by small groups of security experts often labeled as 'paranoid' or 'rigid'. Today, IA is well-known by most individuals involved with Government contracts ranging from high-level executives to engineers of many disciplines. Many have sought information on IA processes through reading papers and attending briefings, however, many questions still loom concerning the nuts and bolts of baking IA into systems being developed. This time, let's forget the four-phase DITSCAP and the five-activity DIACAP and talk implementation.

This paper goes beyond IA processes and addresses how to actually integrate IA requirements into your system. The paper delves deeper into the IA controls using Department of Defense Instruction (DoDI) 8500.2 as an example. It discusses in detail, the technical, administrative, and physical controls required for many systems, summarizes what they mean, and provides guidance on how to implement them. Additionally, the paper covers product selection and what to do if a desired product is not on an approved products list. The paper also addresses the importance of establishing a secure baseline configuration on the products selected prior to software and application development.

Implementing IA in system development is paramount to protecting all information systems from any form of compromise. If left ignored, not only would systems be more vulnerable to attack, they would also not be permitted to operate without obtaining the required Authorization to Operate (ATO). If you are looking for a good read on IA processes, our 2008 I/ITSEC Paper, "DIACAP – Information Assurance Evolved" can be downloaded from the I/ITSEC site; however, if you truly crave knowledge on the nuts and bolts of implementing IA, beyond the process, you want to read this paper.

ABOUT THE AUTHORS

Ms. Misty Piatek is an Associate at Booz Allen Hamilton specializing in Information Systems Security Engineering. She has a Master's in Business Administration from Saint Francis University and a Bachelor's of Science in Computer Science from the University of Pittsburgh in Johnstown, PA. Ms. Piatek is an accomplished Program Manager and IA analyst that has been in the Information Technology field for over 12 years. Ms. Piatek obtained both her Project Management Professional (PMP®) and Certified Information Systems Security Professional (CISSP®) certifications.

Mr. James Newkirk serves as the Deputy to the Director of the Cyber Security Office in the CIO at the Program Executive Office for Simulation, Training and Instrumentation (PEO STRI) in Orlando, FL. He assists in managing the Cyber Security Office which provides support across the $3.5 billion a year organization with over 1100 military, civilian and industry personnel servicing over 335,000 training systems around the world. Mr. Newkirk served in the U.S. Navy and then worked as a contractor for the Army before joining the Army Acquisition Corps as a Government employee and has completed over 12 years of recognized Government service. He holds a Bachelors of Science in Business Administration - Management Information Systems (MIS) from the University of Central Florida.

Implementing Information Assurance – Beyond Process

Misty Piatek
Booz Allen Hamilton
Johnstown, PA
Piatek_Misty@bah.com

James Newkirk
PEO STRI
Orlando, FL
James.R.Newkirk@us.army.mil

SHIFTING FOCUS FROM PROCESS TO IMPLEMENTATION

Understanding the Information Assurance (IA) Certification and Accreditation (C&A) process is very important to achieving the desired outcome; but it only scratches the surface of understanding what really needs done to achieve an Authorization to Operate (ATO). Through outreach efforts, training, articles and presentations, the training and simulation community has learned that IA requirements are planned and enforced from program inception. The community has also learned about the Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) by which IA is integrated into the System Development Lifecycle (SDLC). More information on implementing the DIACAP process can be found in the 2008 I/ITSEC Paper, "DIACAP – Information Assurance, Evolved" (Newkirk & Piatek).

There has been a shift in the type of knowledge that the training and simulation community is craving. Questions are evolving from simple process-based questions to more complicated questions regarding understanding the nuts and bolts of implementing IA requirements. Common questions include:

- What technologies and devices must be a part of the system?
- What products can be used in the system?
- What technical configuration changes need implemented on system components?
- What policies and documents are required?

If you have similar questions, roll up your sleeves and get ready to learn the details on how to implement IA.

THE IA CONTROLS

The IA controls/requirements for Department of Defense (DoD) systems with a classification level of Top Secret and below are documented in DoD Instruction (DoDI) 8500.2. The controls are broken out into eight subject areas as summarized in Table 1 (DoD, 2003, p.49). Assignment of individual controls is based on the Mission Assurance Category (MAC) and Confidentiality Level (CL) of the system. The MAC level can be either I, II or III with level I being the most mission critical with the highest integrity and availability needs. The CL can be either Classified, Sensitive or Public.

Table 1. IA Control Subject Areas

Subject Area Name	# Controls in Area
Security Design and Configuration	31
Identification and Authentication	9
Enclave and Computing Environment	48
Enclave Boundary Defense	8
Physical and Environmental	27
Personnel	7
Continuity	24
Vulnerability and Incident Management	3

This paper sheds light on what many of these controls mean. The logical grouping of our control explanations divert slightly from the subject areas called out in DoDI 8500.2 and Table 1 above and are based on how the controls are implemented.

The controls levied by DoDI 8500.2 can fit into three main categories: technical, administrative, and physical. Technical controls leverage technology in the form of hardware, software, and firmware that protect data and information systems. A few examples of technical controls include encryption, auditing tools, and anti-virus. Administrative controls focus on the human element through the development of policies, processes, training and awareness, etc. to prevent or respond to unauthorized access, as well as, other disruptive events. Physical controls use means such as fences, locks, badges, and guards to prevent or detect intrusions into protected areas.

TECHNICAL CONTROLS

The technical controls account for a large representation of the DoDI 8500.2 controls. These technical controls help influence and shape the design of the system by determining what types of IA technologies are required to protect the system. The technical controls also define how systems should be configured to reduce the risk of the system. The technical controls discussed in this section do not represent an all inclusive list due to the large number of technical controls and the limited size of this paper.

Boundary Protection

One of the first steps in designing the system is to define the system's boundary or boundaries. External interfaces (anywhere data potentially leaves/enters the boundary) must be defined, understood and documented. These interfaces must be protected using devices such as securely configured routers, firewalls and Intrusion Detections Systems (IDS). Special considerations must be given to Controlled Interfaces (CIs), such as, Cross Domain Solutions (CDS). A CI is an interface that provides connection between two boundaries with different classification levels. In order to connect boundaries through a CI, an accredited network guard must be deployed and guidance from Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6211.02C must be followed (CJCS, 2008). Guards are expensive, timely to deploy and networks requiring them are looked at under a microscope to ensure Classified data does not bleed over to the low side of the network.

The existence and integration of connections to the Internet are dependent on the CL of the system. Classified systems do not allow for any connection to the Internet. Sensitive systems can accommodate an internet connection, but it must be physically isolated from the system and located within a Demilitarized Zone (DMZ). Public systems have few restrictions regarding internet presence.

Instructions for restart and recovery of boundary protection devices must be documented and available. This provides for the ease of recovery from unexpected events. MAC I and II systems require the security support structure providing boundary protection to be partitioned and maintain separate execution domains (e.g. a firewall providing protection for the boundary cannot also be used for non-security purposes such as hosting a web application or for general computing use). These network devices must also be physically secured in a room with access control mechanisms in place to prevent unauthorized access.

Boundary protection devices, just like all other hardware, software, and firmware products, must be selected from an approved list of products.

Product Selection

When choosing products for the system, many considerations must be made. Selected IA and IA enabled Commercial off the Shelf (COTS) or Government off the Shelf (GOTS) products must have undergone or be in the process of undergoing evaluation by the National Information Assurance Partnership (NIAP). A helpful resource for information on approved products can be found at the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) web site (www.niap-ccevs.org).

However, finding a product on the list is not the only consideration. The robustness level for which the product has been evaluated and approved is also important. Security Robustness is defined as the strength of a security function, mechanism, service or solution, and the assurance that it is implemented and functioning correctly (NIAP, 2009). There are three levels of robustness for consideration: high, medium, and basic.

- High robustness provides for the most stringent protections and rigorous security countermeasures. High robustness is used to protect highly valued assets, assets in hostile environments, or both.
- Medium robustness provides for layering of additional safeguards above good commercial practices. Medium robustness is considered for environments less hostile than those of high robustness, as well as, for lesser valued assets.
- Basic robustness equates to best commercial practices where protection requirements are minimal.

The required robustness level of the selected product is directly related to the CL of the system (DoD, 2003).

- Classified systems with data that traverses systems of a lower classification level require the use of high robustness products;
- Sensitive systems require the use of medium robustness products if the information transits public networks or the system is accessed by individuals that don't have authorization to access all the information on the system; and
- Public systems require the use of basic robustness products.

So how does robustness impact your selection of products? The answer: When looking at the NIAP-CCEVS Validated Products List (VPL) or Products in Evaluation List, you will need to look at the column titled "Conformance Claim". In this column you will see references to Evaluation Assurance Levels (EALs):

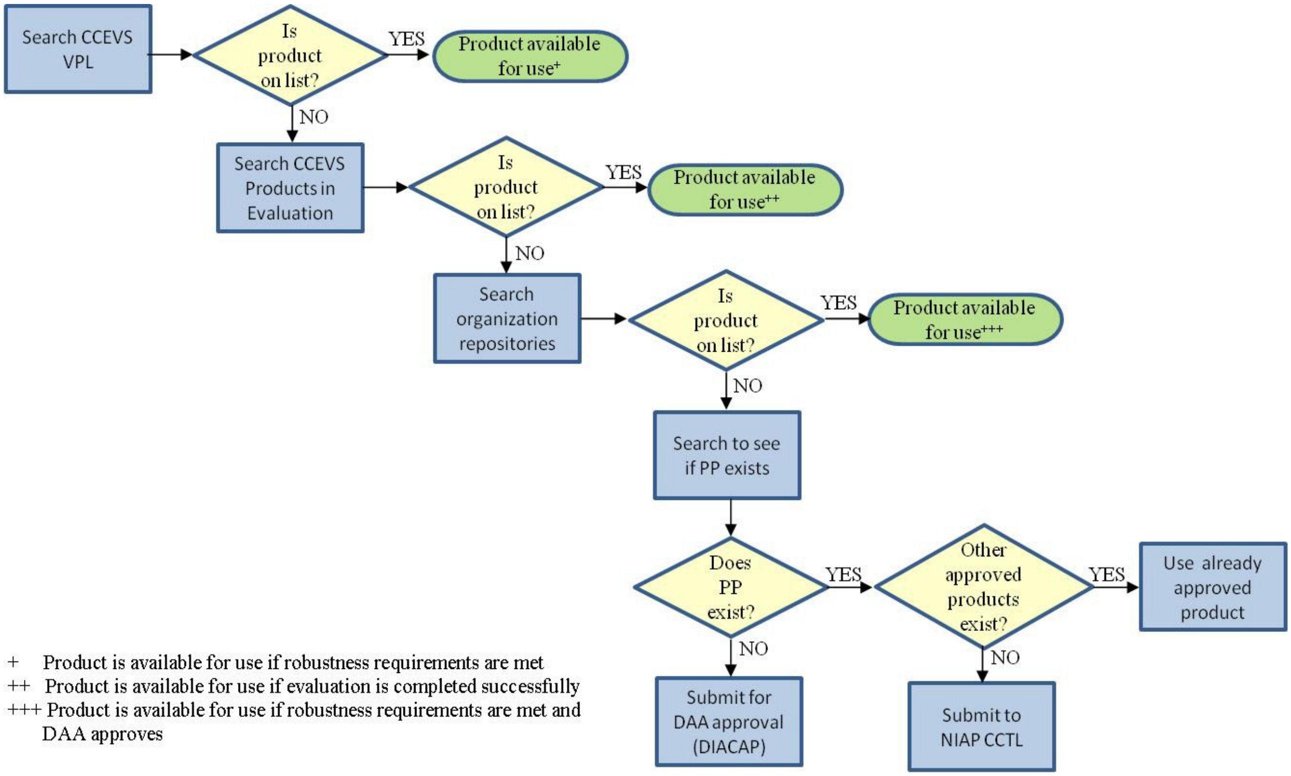
- Basic Robustness requires a EAL ≥ 2,
- Medium Robustness requires a EAL ≥ 4 and
- High Robustness requires an EAL > 6 (NIAP, 2009).

What if the product I need is not on the list?
If a product is not currently on the CCEVS VPL, then the product should be searched for on the CCEVS Products in Evaluation list. If the product is found on this list, it can be used with the understanding that selecting a product undergoing evaluation poses the risk of selecting and buying a product that may ultimately fail the evaluation. If this occurs, an approved product must be selected as a replacement, resulting in costly re-design and implementation.

There is another search you can perform if the desired product is not on the NIAP-CCEVS VPL. A repository of other approved products is kept by different service organizations such as the Army, Navy, Air Force and Marines. These repositories contain information on products/systems accredited and approved for use by the organization's Designated Approval Authority (DAA). If the product is in the organization's repository, it should be approved for use; however, the DAA has the final approval and should be consulted. Repositories include:

- Navy - Department of Navy Application and Database Management System (DADMS),
- Air Force – Enterprise Information Technology Data Repository (EITDR),
- Army – Army Portfolio Management Solution (APMS) and
- Marines - Marine Corps Enterprise Software Portfolio.

If the product isn't listed in one of the above repositories, the answer becomes more complicated. The approach for this product is based on whether or not a Protection Profile (PP) exists for the technology area (IDS, Firewall, etc.) and whether or not there are any other products available that have been evaluated against the PP. If an alternate approved product exists, it should be used. If there aren't any approved products listed for the technology area and a PP does exist, you must request that the vendor of the product submit their product for evaluation through a NIAP Common Criteria Test Lab (CCTL). If a PP doesn't exist, then you must request the vendor submit their product for evaluation at the DAA level. Figure 1 summarizes the workflow for selecting products for use.


Search CCEVS VPL
Is product on list?
YES
Product available for use+
NO
Search CCEVS Products in Evaluation
Is product on list?
YES
Product available for use++
NO
Search organization repositories
Is product on list?
YES
Product available for use+++
NO
Search to see if PP exists
Does PP exist?
YES
NO
Other approved products exist?
YES
Use already approved product
NO
Submit for DAA approval (DIACAP)
Submit to NIAP CCTL

+ Product is available for use if robustness requirements are met
++ Product is available for use if evaluation is completed successfully
+++ Product is available for use if robustness requirements are met and DAA approves

Figure 1. Product Selection Workflow

Government Furnished Equipment (GFE) and Custom Applications

Government Furnished Equipment (GFE) is often another consideration as part of your architecture. It typically comes in the form of a custom developed hardware/software product that is required for use. GFE is required to undergo its own C&A effort by the organization developing the product. A Memorandum of Agreement (MOA) can be used to note the requirement to use the GFE as part of the architecture.

Other custom developed applications are also a common consideration. These applications can be accredited as part of the system by ensuring:
1. The application design and functionality is fully documented to include: roles and permissions; information on the type and format of data that is processed, imported, and exported; validation methods and results; and a lifecycle support plan.
2. The Application Security and Development Security Technical Implementation Guide and software quality best practices are followed (DISA, 2008).
3. The application is developed on a securely configured platform and doesn't use any restricted ports, protocols or services.

Other Product Selection Considerations

Mobile Code and Public Domain Software are discouraged but can be used under certain circumstances. DoDI 8552.01 (DoD, 2006) categorizes mobile code into 3 main types. The three types are based on what the mobile code can access or perform during execution. Approval for use will depend on:

- the type of mobile code,
- whether or not it is signed with a trusted code signing certificate and
- how it was obtained.

Even if mobile code is not intended for use on the system, further burden of proof that it isn't installed is required. For example, the Defense Information Systems Agency (DISA) Gold Disk can be used to scan the system and show all applications residing on the system. That scan should prove that only approved applications are on the system and mobile code is not present, as expected.

Open source software must comply with all of the same IA requirements as any other product. If the software libraries are supported with a limited warranty or no warranty at all, an alternative solution must be selected. If no alternative is available, the DAA can approve its use if it is critical to the success of the mission. Freeware and shareware are prohibited unless the DAA deems it critical to the success of the mission.

Establishing the Secure Baseline Configuration

Now that your products have been selected, they need to be configured according to configuration guides. This is also referred to as establishing a secure baseline configuration.

The DoDI 8500.2 (DoD, 2003) IA control "Security and Design Configuration - Configuration Specifications (DCCS)" requires that all IA and IA enabled products be configured in accordance with configuration guidance such as the Security Technical Implementation Guides (STIGs) provided on the DISA website (http://iase.disa.mil/stigs). Configuration guides provided by the NSA System Network and Attack Center (SNAC) can be used in the absence of a STIG, these guides can be found on the NSA website (http://www.nsa.gov/ia/guidance/security_configuration_guides). In the event that STIG or SNAC guidance is not available, best security practices should be used.

Configuration guides used to establish the secure baseline configuration take you through a series of steps and configuration changes that ensure the system has the minimum security configurations in place; these configurations include but are not limited to:

- appropriate service packs and patches are installed,
- necessary registry key edits are made,
- Access Control Lists (ACLs) are configured properly,
- auditing roles and permissions are properly configured,
- password policy is properly set/enforced, and
- messaging services are disabled or properly configured.

Tools and scripts are available to expedite the configuration process on some platforms. For example, approved Windows Operating Systems (OS) can run the DISA Gold Disk to automate the process of configuring the OS. Security Readiness Review (SRR) Evaluation Scripts can also be used to assist with the configuration of applications such as Unix-like OSs, Virtual Memory System (VMS), Oracle and more.

Once the secure baseline configuration has been achieved, an image of the devices should be created in order to provide backup for quick restoration of the system. Other special procedures required to restore the system should also be recorded to facilitate recovery. It is important to understand that development of applications should not occur on the development station until the baseline configuration has been established. Development prior to the baseline configuration can lead to increases in schedule, budget and frustration due to the fact that the application being developed may function differently once the secure baseline configuration is established.

Ports, Protocols and Services Management (PPSM)

The use of acceptable ports, protocols and services (PPS) is another important consideration in the design and implementation of the system. IA control "Security Design and Configuration - Ports, Protocols and Services (DCPP)" requires that the system comply with guidance set forth for the use of ports, protocols and services (DoD, 2003). The guidance is based on DoDI 8551.1 (DoD, 2004) and includes reference to the PPS Category Assurance List (CAL) (DISA, 2009).

This PPS CAL catalogs various ports, protocols and services and highlights them in three colors, which represent their assurance level category. PPSs highlighted in red are considered low assurance and unacceptable for use unless approved by the Defense Information Systems Network (DISN) DAA under specific conditions and restrictions given no other feasible alternative exists. PPSs highlighted in yellow are designated as medium assurance and can be implemented only if additional mitigation strategies are approved by the DISN DAA and employed. PPSs highlighted in green reflect high assurance and best practice for use on DoD systems. Some examples of common PPSs that should be avoided include: File Transfer Protocol (FTP), Internet Relay Chat (IRC), Remote Login (LOGIN), Network Virtual Terminal Protocol (TELNET), SHELL, and Finger (DISA, 2009). More secure alternatives exist and can be used with acceptable mitigation strategies.

All PPSs used within the boundary must be documented in the System Security Plan (SSP) or Information Security Plan (ISP). Any PPSs not required for operation by the system must be disabled. This supports the IA principal of least privilege and reduces the system's risk of exploitation. Unnecessary open or enabled PPSs will be detected during test and evaluation and will be reported as findings.

Instant Messaging

Instant Messaging (IM) within an enclave can be used as long as it performs an authorized and official function. The IM products selected for use must be approved and configured according to the IM STIG (DISA, 2009) and in compliance with the PPS CAL. File sharing through IM is prohibited given its ability to bypass security and auditing policies within the enclave. The IM server is required to be located behind the firewall and the IM gateway server must be located in the DMZ. Any unused IM Services must be disabled.

Implementing an IM capability within the boundary carries many policy and documentation requirements. Username and passwords policies apply, as do auditing and logging, usage behavior, and many others. The IM architecture will also need to be documented in detail as part of the C&A package.

IM clients, servers or gateways are strictly prohibited from communicating with any public network. IM traffic within the enclave boundary is not permitted to leave the boundary, and IM traffic from outside the enclave boundary is not permitted into the enclave boundary.

Encryption

Encryption requirements address two states of data: (1) Data at Rest (DAR) and (2) Data in Transit. Encryption requirements are levied based on:

- the state of the data,
- the classification level of the data,
- the classification level of the networks in which data traverses and
- the "need to know" of the users accessing those networks and network devices.

Encryption - Data at Rest

DAR refers to all data in computer storage including hard disks, Compact Discs (CDs), Digital Versatile Discs (DVDs), Universal Serial Bus (USB) drives, cell phones, and other removable storage media.

For systems with a CL of Classified, it is suggested that Classified, non-Source and Methods Intelligence (non-SAMI) information be encrypted using FIPS 140-2 compliant cryptography; however, the decision is ultimately left to the data owner on whether or not to require data at rest encryption in this instance. If the enclave contains SAMI information and can potentially be accessed by individuals lacking clearance for access to SAMI information, then NSA-approved cryptography is required to encrypt all the SAMI data. For systems with a CL of Sensitive, the information owner can determine if Sensitive data is to be encrypted using FIPS 140-2 cryptography. Data that has been reviewed and approved for public release does not require encryption. However, it is important to note that all Unclassified DoD information is treated and protected as Sensitive until it is reviewed and approved for release in accordance with DoD Directive 5230.9 "Clearance of DoD Information for Public Release" (DoD, 1996).

DAR - Passwords

All the above information holds true for data at rest; however, there are a few caveats. Passwords on Unclassified systems or Classified systems that don't contain any SAMI data must be stored using FIPS 140-2 compliant cryptography. Passwords on Classified systems that contain SAMI data with users that don't possess the appropriate clearances for SAMI data must be stored using NSA approved cryptography.

DAR - Mobile Devices

Mobile devices such as laptops, removable hard drives, Personal Digital Assistants (PDAs), cell phones and other portable and removable media increase the risk of data exposure. Given this serious risk, the DoD released the DoD Policy Memorandum "Encryption of Sensitive Unclassified Data at Rest on Mobile Computing Devices and Removable Storage Media" (DoD, 2007) stating that all Unclassified data stored on mobile devices and removable media that has not been specifically approved for public release must be treated and protected as Sensitive data, thus requiring it to be stored using FIPS 140-2 compliant cryptography (DISA, 2008).

Encryption – Data in Transit

Data traversing a network is referred to as Data in Transit. Additional requirements are considered for data in transit and are based on the classification of the data, the classification of the network it is traversing, and the "need to know" of the users accessing the network. All Classified networks require the core backbone to be encrypted using NSA-approved Type I cryptography. Any Classified data that is transmitted across a network that is cleared to a lower classification level than the data itself (for example, Top Secret data traversing a Secret backbone) must be encrypted in a separate tunnel with NSA-approved cryptography. If the data is transmitted over a network with the same classification level, but not all users of the network have the appropriate "need-to-know", the data must be encrypted in a tunnel using FIPS 140-2 compliant cryptography. Any SAMI information in transit across a network at the same classification level must be separately encrypted in a tunnel using NSA-approved cryptography.

In the event remote access is required and approved, encryption requirements are applicable. If the remote user is accessing Sensitive data the session must be encrypted using FIPS 140-2 compliant cryptography. Remote access to Classified systems is seriously discouraged and rarely approved; however, if it is required, the session must be encrypted with NSA approved cryptography. Additionally, in wireless networks all Unclassified, Sensitive information must be encrypted using FIPS 140-2 compliant cryptography. Table 2 provides a simplified summary of encryption requirements for both DAR and Data in Transit.

Table 2. Summary of Encryption Requirements

Type of Data	FIPS 140-2	NSA
DAR – Public Releasable	-	-
DAR – Sensitive	X[+]	
DAR – Classified/no SAMI	X[+]	
DAR – Classified/SAMI		X
DAR – Passwords on Sensitive/Public network	X	
DAR – Passwords on Classified/no SAMI	X	
DAR – Passwords on Classified/SAMI		X
DAR – Mobile Devices	X	
Transit – Classified backbone		X
Transit – Data higher classification than backbone		X
Transit – Data where users lack "need to know"	X[++]	
Transit – SAMI		X[++]
Transit – Remote Access to Sensitive data	X	
Transit – Remote Access to Classified data		X
Transit – Wireless networks with Sensitive data	X	

[+] Data Owner decides the requirement for encryption
[++] Data is tunneled within NSA encrypted backbone

Identification, Authentication and Access Control

Identification, authentication, and access control is another large area of consideration when designing and implementing systems. Identification and authentication serve as a foundation for access control. Once a user identifies himself/herself, the user's identification factors are verified through the process of authentication. Once authenticated into the system, access control mechanisms are used to determine what the user has access to based on attributes, roles, and permissions.

Identification and Authentication applies to humans, devices and services. MAC I and II systems require that users be authenticated via a DoD Public Key Infrastructure (PKI) Class 3 or Class 4 certificate and a hardware security token or using a NSA-certified product. A smart card and the Common Access Card (CAC) are examples of the hardware security token that contain the certificates. MAC III systems only require a Class 3 certificate.

Group authenticators to applications/networks may be used if they are used in conjunction with an individual authenticator based on DoD PKI. If they are not based on DoD PKI, approval must be obtained from the DAA. If a password is used in conjunction with a personal identifier, the password must meet complexity requirements. For example, passwords must be at least 14 characters long with a mix of upper case letters, lower case letters, numbers and special characters. Expiration and password re-use must be configured in accordance to DoD or organization policy (whichever is more stringent). All passwords must be encrypted both at rest and in transit. Classified systems require testing/password cracking to be performed in order to ensure password strength measures are followed and effective.

Logon attempts must be strictly controlled to combat brute force attacks and other attempts to gain unauthorized access. Systems must be configured to lock accounts after either a set number of consecutive unsuccessful logon attempts or a set number unsuccessful logon attempts within a decided period of time. For Classified systems, after successful logon, the date/time of the last logon must be displayed including the location of the logon and the number of unsuccessful logon attempts since the last successful logon. This will help the user identify any suspicious, unauthorized activity using their account. All DoD systems, regardless of MAC or CL, must display the DoD Warning Message in compliance with the DoD Memorandum Subject: Standard Mandatory DoD Notice and Consent Banner (DoD, 2008).

There are two principles in IA that apply heavily to access control. These principles are: 1) the Principle of Least Privilege and 2) the Principle of Separation of Duties. The principal of least privilege supports providing the least amount of access/permissions necessary for any user or device. This limits a user's ability to cause intentional or unintentional damage. This principal is supported by requiring any changes to system configuration or production code to be performed by authorized individuals through privileged accounts. Privileged users, such as administrators, must have separate accounts to carry out privileged functions. They must have non-privileged accounts to perform their non-privileged, day-to-day functions.

The principal of separation of duties supports separating jobs/functions to ensure a single individual does not have the power to defraud a system. Collusion would be required to accomplish such an attempt. For example, the administrator and auditor roles must use distinct accounts and be assigned to different individuals. This ensures that a single user/administrator cannot cover their tracks by modifying or destroying audit data after intentional or unintentional damage occurred on the system.

Audit

Auditing can be viewed as both a technical and administrative function. Auditing in the form of using technology and system configurations to ensure user actions are logged and stored is a technical function. Auditing assists in the identification and investigation of unauthorized activity. Systems that are MAC I, II, or Classified require that automated, continuous on-line monitoring and audit trail creation is implemented and immediately alerts personnel of suspicious activity. The automated system must have the capability to automatically disable the system during serious situations. MAC III, Sensitive or Public systems only require manual, periodic review of audit data. Audit logs must record the success/failure of the following:

- logon events,
- account management,
- directory Service access,
- account logon events,
- object access,
- policy change,
- privileged use,
- process tracking and
- system events.

As briefly stated earlier, it is important that the audit data be protected from unauthorized access and modification. A separate auditor role must be established for auditors and ensure separation of duties by excluding administrators and other privileged users from inclusion into the auditor group.

Audit records must be backed up at least weekly onto other system media for MAC I and II systems. MAC III systems should also be backed up routinely based on best practices, but a specific timeframe requirement is not specified in DoDI 8500.2.

Virus Protection

All IA and IA-enabled devices, such as servers, workstations and mobile devices, must deploy an approved Anti-Virus solution capable of receiving automatic updates. In the event Anti-virus is determined to be a detriment to the function and performance of the device, thorough testing must be performed to prove degradation to performance exists and negatively impacts the mission (burden of proof is required) and documentation must be updated accordingly. The ultimate decision lies with the DAA as to whether or not the absence of Anti-Virus on the device is acceptable; however, obtaining this type of approval isn't common.

ADMINISTRATIVE CONTROLS

As described earlier, administrative controls focus on the human element through the development of policies, processes, training and awareness programs, etc. to prevent or respond to unauthorized access and other disruptive events. Many DoDI 8500.2 controls require the development, documentation, implementation and audit of policies, procedures, standards, guidelines and other documentation. In this section, you will learn about many of these requirements to include the majority of the documentation required.

Configuration Management

Configuration Management (CM) plays a key role in IA. CM is paramount throughout the SDLC in understanding and documenting the ever-changing functional and physical attributes of the system. CM helps individuals understand how the system has changed, who authorized the changes, when changes were implemented, etc. All DoD systems required to comply with 8500.2 controls must follow a CM Plan. The CM Plan must formally document CM roles and responsibilities to include the establishment of a Configuration Control Board (CCB). MAC I and II systems require the Information Assurance Manager (IAM) to participate as a member of the CCB in order to assess IA impact of any proposed changes. The CM Plan also addresses the processes for:

- reviewing and approving system changes and documentation,
- testing system changes, patches and updates prior to deployment, and
- verifying that the CM process is followed and effective.

All documentation discussed under administrative controls is required to be managed under the applicable CM Plan.

IA Architecture Documentation

Documentation detailing architectural information of the system is required in order for the system to be properly designed, implemented, and maintained, as well as, for the DAA to be able to make an informed decision on whether or not the system maintains an acceptable level of risk in order to receive its ATO.

Much of this documentation is part of the DIACAP Package and is located in the Information Security Plan (ISP). However, other pieces of supporting documentation may contain the information and can be referenced in the ISP. Documented architecture information in the ISP must include:

- Appointment of IA roles, responsibilities and criteria, such as clearances, training and certifications. This includes identification of the DAA, Certification Authority (CA), User Representative (UR), and IAM
- Detailed architecture boundary diagrams highlighting external and controlled interfaces and the protection mechanisms in place at each interface
- Hardware and software baseline inventories
- Detailed data flow diagrams
- Description of data and corresponding sensitivity/classification levels
- User roles required for access control and privileges assigned to each
- Unique security requirements
- Use of mobile code, impact assessment and mitigations
- Use of public domain software, impact assessment and mitigations
- Use of system libraries
- Protection mechanisms for DAR and data in transit
- Ports, Protocols and Services in use
- Restoration priority of subsystems, processes and information

Hardware and Software Baseline Inventories

Both a hardware and software baseline inventory must be documented and managed under the CM Plan. This information is often found in the ISP; however, these baseline inventories must also be separately stored in a fire rated container in the event the main documentation is destroyed.

Information Assurance Vulnerability Management Plan (IAVMP)

An Information Assurance Vulnerability Management Plan must document how IA Vulnerability Alerts (IAVAs), IA Vulnerability Bulletins (IAVBs), and IA Technical Advisories (IATAs) are received, evaluated for applicability, tracked, and implemented. The plan must include a detailed process for downloading and installing patch files on test systems in a mirrored lab environment, and patching the deployed systems if no issues are found.

Incident Response Plan

An Incident Response Plan must be developed to identify who incidents are reported to and what procedures to follow once and incident has occurred. The plan identifies members of the incident response team and outlines their roles and responsibilities. It will also define a user training program for identification and response to incidents. The Incident Response Plan is required to be exercised every six months for MAC I systems and annually for other systems.

Policies and Procedures

Many policies and procedures are required for the secure operation of systems. Many times these policies and procedures are already in place at the site in which the system will be deployed. These policies can be "inherited" and referenced as part of the system's documentation. If the policies and procedures do not exist or are not stringent enough, modification or creation of new policies and procedures is required. Proof must be provided to show that the policies do formally exist in writing and are being followed. Validation methods typically used include review of documentation and the performance of interviews. Required policies include:

- Personnel policies such as hiring, suspension and termination procedures
- Acceptable use policy for the system
- Account Management procedures to create, modify and delete both privileged and non-privileged accounts. The procedures also detail in accordance with DoD policy how often account lists are reviewed and when dormant accounts are suspended. In many instances the IAM is required to track all privileged accounts.
- Data handling and dissemination for marking and labeling in accordance with DoD 5200.1R
- Backup and recovery procedures

Disaster Recovery, Contingency and Continuity of Operations Plans

Plans must be developed that provide information on what to do in the event of a disaster or disruption in availability of the system or sub-system. These plans must identify mission and business essential functions and their priority for restoration. These plans detail or reference procedures for the backup and restoration of hardware and software. Operation and timeliness of alternate sites is based on MAC level.

- MAC I systems require an identical geographically distanced "hot site" be maintained in parallel to the main system. The hot site must immediately be available for operation without loss of data or function. The plan must be fully tested semi-annually.
- MAC II systems require that an alternate site be identified in the event a disaster or disruption occurs, allowing all business and mission essential functions to resume within 24 hours. Plans must be exercised annually to verify their effectiveness.
- MAC III systems require an alternate site that permits the partial restoration of mission or business essential functions within 5 days of a disaster. Plans must be exercised annually to verify their effectiveness.

Backup copies of critical software, data, restoration procedures, and audit trails must be stored in a fire-rated container at a separate location. The availability of spare parts is also a consideration in the continuity of operations. Requirements for the availability of spare parts is based on MAC level and ranges from immediate availability for MAC I to within 24 hours for MAC III systems.

Other Required Documentation

A few additional pieces of documentation are required in order to get an ATO for the system; they include:

- MOAs – Required for all interconnecting systems and/or boundaries. Also required for any IA or IT services required for operation of the system.
- Documented proof showing IA as a budgeted line item for the program
- Software development plans and software test plans
- IA test plans and procedures
- IA test results (DIACAP scorecard)
- IA mitigation strategies (Plan of Actions and Milestones (POA&M))

PHYSICAL CONTROLS

Physical controls protect, monitor and control the environment of the facilities. Controls often times include security guards, locks, cameras, fences, badges, and more. Physical controls may be inherited from the site at which the system is to be installed. Some of these controls are implemented with technology, while others require documentation and implementation of policies and procedures required to secure the facilities. Personnel must be trained in all facets of environmental control. Physical controls are not detailed in this paper but can be found in DoDI 8500.2 (DoD, 2003). Some examples include:

- Automated vs. manual fire detection, inspection and suppression based on MAC level
- Automated vs. manual temperature and humidity controls based on MAC level
- Emergency lighting
- Voltage regulation
- Positioning of data displays, such as, monitors to deter shoulder surfing (looking over one's shoulder to access data)
- Data handling and dissemination in accordance with DoD 5200.1R (DoD, 1997)
- Facility guarding, access policies and procedures

CONCLUSION

The road to success in implementing IA is baking IA into the SDLC. IA requirements must be considered at program inception and must be defined early in the acquisition strategy and process. This ensures IA is included in the budget and the Statement of Work (SOW).

Once the program is awarded, the engineering team must identify all applicable IA requirements for the system. Many of the IA requirements are complex and not easily understood. Trained and certified system security engineers should be integrated into the team to provide guidance and system security engineering. Using certified system security engineers is not only a suggestion, but also a requirement mandated by DoD Directive 8570.1, Information Assurance Training, Certification and Workforce Management (DoD, 2004).

REFERENCES

Chairman of the Joint Chiefs of Staff (CJCS), (2008). *Instruction 6211.02C Defense Information System Network (DISN): Policy and Responsibilities.*

Defense Information Systems Agency (DISA), (2008). *Application Security and Development.* Retrieved June 26, 2009 from http://iase.disa.mil/stigs/stig/application_security_and_development_stig_v2r1_final_20080724.pdf

Defense Information Systems Agency (DISA), (2008). *Frequently Asked Questions DoD Policy Memorandum "Encryption of Sensitive Unclassified Data at Rest on Mobile Computing Devices and Removable Storage Data.* Retrieved May 27, 2009 from http://iase.disa.mil/policy-guidance/faq_dar_encryption_policy_memo_18mar08_update-6_final.doc

Defense Information Systems Agency (DISA), (2009). *Instant Messaging Checklist.* Retrieved April 23, 2009 from http://iase.disa.mil/stigs/checklist/instant_messaging_checklist_v1r2.5.pdf

Defense Information Systems Agency (DISA), (2009). *Ports, Protocols and Services Management (PPSM) Category Assurance List(CAL) Sorted by Services.* Retrieved April 23, 2009 from http://iase.disa.mil/ports/index.html

Department of Defense, (1997). *5200.1-R Information Security Program.*

Department of Defense, (1996). *Directive 5230.9 Clearance of DoD Information for Public Release.*

Department of Defense, (2004). *Directive 8570.1 Information Assurance Training, Certification and Workforce Management.*

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

Department of Defense, (2004). *Instruction 8551.1 Ports, Protocols and Services Management (PPSM).*

Department of Defense, (2006). *Instruction 8552.01 Use of Mobile Code Technologies in DoD Information Systems.*

Department of Defense, (2007). *Memorandum: Encryption of Sensitive Unclassified Data at Rest on Mobile Computing Devices and Removable Storage Media.*

Department of Defense, (2008). *Memorandum: Policy on Use of DoD Information Systems – Standard Consent Banner and User Agreement.*

National Information Assurance Partnership (NIAP). *Protection Profiles Frequently Asked Questions.* Retrieved April 23, 2009, from http://www.niap-ccevs.org/cc-scheme/faqs/pp

Newkirk, J. & Piatek, M. (2008). *DIACAP – Information Assurance, Evolved.*