DIACAP – Information Assurance, Evolved

Ms. Misty Piatek
MTS Technologies, Inc.
Johnstown, PA
piatekm@mtstech.com

Mr. James Newkirk
PEO STRI, Office of Information Assurance
Orlando, FL
james.r.newkirk@us.army.mil

ABSTRACT

Many inconsistencies and misconceptions exist throughout government and industry concerning what Information Assurance (IA) is and why it is important for training systems. What began as a vague concept creating a great deal of confusion has evolved into a mature, streamlined process resulting in increased levels of understanding and preparedness.

The paradigm has shifted; Program Managers and Engineers are now much more aware of the security requirements their systems must comply with to ultimately obtain authorization to operate. Throughout this familiarization process, which included awkward acronyms, cumbersome processes (DITSCAP), and antiquated artifacts (SSAA), the IA process evolved into a new breed: DIACAP. Immediately following this conversion, many complaints surfaced expressing well-founded concerns. If this question lurks in your mind: "I just started understanding DITSCAP, now there is the DIACAP, what does this mean to me?", then you will want to read this paper.

This paper responds directly to those concerns. It analyzes the DIACAP and addresses how the DIACAP ties into the program and acquisition schedule from cradle to the grave. The paper documents two proven IA methodologies, the preferred "Baked-in" approach and the alternative "Bolted-on" approach. Additionally, the five DIACAP activities, accreditation maintenance requirements, development of various artifacts, and identification of necessary tasks to ensure success are discussed. The paper increases understanding of the DIACAP evolution and identifies positive outcomes of each, including efficiencies realized, roles defined, more pertinent artifacts, and the change in type- vs. site-based accreditations.

IA is an ever-critical component that needs to be fully integrated into all information systems, which ensures that confidentiality, integrity, and availability are "Baked-in" and inherent in training devices. This paper will prove that the IA process has evolved into a proven, streamlined implementation ensuring training systems effectively and securely support three crucial Warfighter objectives: Learn. Train. Win!

ABOUT THE AUTHORS

Ms. Misty Piatek is the Manager of Information Assurance (IA) East at *MTS Technologies, Inc.* 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 10 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 Information Assurance Program Manager (DIAPM) in the CIO at the Program Executive Office for Simulation, Training and Instrumentation (PEO STRI) in Orlando, FL. He assists in managing the IA Office, which provides IA support across the $2.2 billion per-year organization with over 1,025 military, civilian, and industry personnel servicing over 334,000 training systems around the world. Mr. Newkirk served honorably in the US Navy and worked as a contractor for the Army before joining the Civil Service and completing over 10 years of recognized Government service. He holds a Bachelor's of Science in Business Administration in Management Information Systems (MIS) from the University of Central Florida.

DIACAP – Information Assurance, Evolved

Ms. Misty Piatek
MTS Technologies, Inc.
Johnstown, PA
piatekm@mtstech.com

Mr. James Newkirk
PEO STRI, Office of Information Assurance
Orlando, FL
james.r.newkirk@us.army.mil

HOW DID WE GET HERE?

Without a doubt, Information Assurance (IA) has been evolving quickly over the years; and yet, no end is in sight. IA's roots may be traced back as early as the 1950s, when it supported the mission of preserving confidentiality and protecting against the capture and analysis of electromagnetic radiation emanations. Three decades later, the 1980s brought us additional developments including standards and policies such as: Federal Information Processing Standard (FIPS) 102 for Certification and Accreditation (C&A) of applications; the Orange Book's computer security guidance; and the Computer Security Act of 1987, which called for the development of standard security practices, minimum requirements, and security training programs for users of federal systems.

In 1997, the Department of Defense (DoD) unveiled a cumbersome IA process, the DoD Information Technology Security Certification and Accreditation Process (DITSCAP). It took many years for the DITSCAP to become engrained into the development of our systems. Finally, after a decade of use, awareness has increased to a level where most individuals understand that IA is a requirement, even if they don't know how to fully integrate it. No matter how detailed the understanding, the message has become clear; in order to connect and/or operate, fielded systems must obtain an Authorization to Operate (ATO). Additionally, to further ensure the implementation and compliance of security requirements, in 2002, Title III of the E-Government Act, better known as the Federal Information Security Management Act (FISMA), brought forth much more stringent computer security requirements by mandating annual audits of government systems.

The past ten years of implementing IA as we knew it changed on November 28, 2007 when the DoD replaced the DITSCAP with the new Defense Information Assurance Certification and Accreditation Process (DIACAP). The major process change has left individuals with many questions. The most common questions include: "I just started understanding the DITSCAP, now there is the DIACAP, what does it mean to me?" and "When is IA going to end?" This paper is intended to help you understand what the change means. IA is and will continue to be a part of the development process throughout the system's lifecycle as a key part of helping protect the way the DoD learns, trains, and ultimately wins.

DIACAP OVERVIEW

The DIACAP [8510.01] cancels the DITSCAP [5200.40], the DITSCAP Manual [8510.1-M], and the interim DoD IA C&A guidance that was put into effect in July 2006. The DIACAP does not enhance the DITSCAP, but rather, completely replaces it with an entirely new methodology of the C&A process. One of the largest influences of the DIACAP is the move towards the globally interconnected enterprise known as the Global Information Grid (GIG). The realization of the GIG and desired levels of net-centricity require that the IA process be more streamlined and the status of systems be more visible to all levels of their major stakeholders. The DIACAP supports and categorizes information systems (ISs) into four GIG Mission Areas:

- Enterprise Information Environment Mission Area (EIEMA)
- Business Mission Area (BMA)
- Warfighting Mission Area (WMA)
- Defense Intelligence Mission Area (DIMA)

Although it seems intimidating to learn an entirely new process, the DIACAP brings forth many welcomed changes including:

- A more streamlined IA process
- Increased visibility of systems and their accreditation statuses
- Additional roles and responsibilities
- Elevated accreditation authority and responsibility
- Increased focus on the technical controls
- A more consistent standardized approach
- Further consideration for the decommissioning of a system

- More stringent annual testing requirements
- Changes in artifacts resulting in reduced paperwork.

These changes are further explained and brought to light throughout this paper.

INITIATION OF THE IA PROCESS

We have seen the IA process initiated at various times during the system acquisition lifecycle. When IA is started after system design and development are complete, the implementation is referred to as the "Bolted-On" approach. The preferred approach, "Baked-In," refers to integrating the IA program and ensuring that security engineering is a discipline that is integrated into the overall system engineering process at the inception of the program. This approach ensures that IA requirements drive the overall system requirements and are mapped all the way through the design, development, deployment, maintenance, and decommission of the system.

Bolted-On Approach

The Bolted-On approach is prevalent in legacy systems or systems whose IA requirements were not explicitly identified in the overall requirements of the program. Implementation of IA late in the System Development Lifecycle (SDLC) leads to many challenges and increased frustrations and costs. Challenges begin early on when the realization of needing an ATO sets in. Achieving an ATO takes time and money, both of which, in most cases, were not incorporated into the schedule or budget of the program.

The Bolted-On approach frequently requires changes to the design and implementation of the system. When IA requirements are levied on a system, not built with security in mind, it commonly results in disrupting the system's functionality and ability to perform its mission. Changes required to fix the system late in the SDLC are much more costly after the system is developed, which again impacts the schedule and budget for the program. In summary, the Bolted-On approach is more expensive than baking IA in early on and results in a less secure system.

Baked-In Approach

IA is now required to be initiated at program inception. The Program Manager must ensure that the appropriate IA requirements are included in contracts, statements of work, and other acquisition documentation. The acquisition strategy for the program must incorporate the resources required to achieve and sustain the ATO until the system is decommissioned. Failure to adequately plan for IA will not result in a waiver to remove the requirements from the program.

The benefits of properly baking IA into the beginning of the SDLC result in the mitigation of design changes and costly re-work due to last-minute realization of requirements. It also results in a more secure system, one designed with security in mind.

KEY DIACAP ROLES AND RESPONSIBILITIES

Key roles and responsibilities for the DIACAP are detailed in DoDI 8510.01. The DIACAP C&A roles are similar to the DITSCAP, except for the addition of two roles, the Principal Accrediting Authority (PAA) and the Senior Information Assurance Officer (SIAO), which resulted in an increased level of independent evaluation and accreditation authority. The addition of the new roles is also representative in part due to the move towards net-centricity implemented through the GIG. The GIG Mission Areas (MA) require an additional representative to ensure that IA is implemented in a consistent form across each MA. Figure 1 illustrates an organizational depiction of the key roles described within this section.

Principal Accrediting Authority

The PAA is the senior official responsible for ensuring that IA is incorporated for ISs in a particular GIG MA. Each GIG MA has its own designated PAA. The PAA establishes guidelines to facilitate consistent accreditation decisions across the MA. The PAA coordinates with the DoD Component Heads to appoint a Designated Approval Authority (DAA) for that component. The PAA provides support and guidance to the DAAs. PAAs may identify a PAA representative to assist in planning and coordinating with the DoD SIAO.

Designated Approval Authority

The DAA is the government official, usually at the General Officer or Senior Executive Service level, that is responsible for determining whether or not a system has met the requirements to receive an ATO.

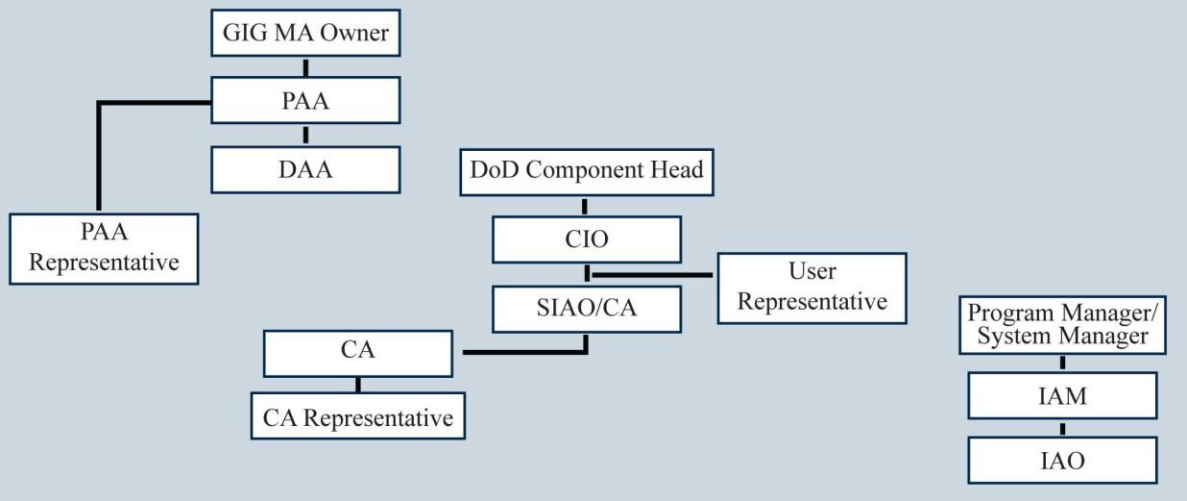

Figure 1. Key DIACAP Roles

The DAA weighs the operational needs and requirements of the system against the security posture and risk it imposes to itself, other systems and other services. In authorizing a system to operate, the DAA ultimately accepts all responsibility for the risk associated with the system that is being accredited. The DAA is also required to ensure that an Information Assurance Manager (IAM) is appointed in writing. Additionally, IAMs are responsible for composing statements of responsibilities for systems under their purview.

Component Chief Information Officer (CIO)

The Component Chief Information Officer is ultimately responsible for the component's IA program. Additionally, he or she ensures that coordination between the DoD Component IA Program, the PAA, and the DAA is present. The Component CIO also ensures that a User Representative is appointed for ISs in accordance with the PAAs guidelines.

Component Senior Information Assurance Officer/Certifying Authority (SIAO/CA)

The SIAO ensures that the appropriate IA controls are implemented for all ISs under the components purview. SIAOs often fulfill the CA role, unless the SIAO chooses to delegate the responsibility to a supporting CA representative. The SIAO/CA formally evaluates the IA posture of the IS and makes a Certification Determination (CD) to the respective DAA. CDs are technical judgments derived from an assessment of system compliance with stated requirements and residual risk based on an evaluation of the DIACAP scorecard and the Plan of Action and Milestones (POA&M) proposed to mitigate residual risk, and the potential impact on the mission and/or other systems/networks.

Program Manager (PM)

The PM is responsible for the IS throughout its lifecycle. PMs must understand IA requirements and allocate appropriate resources (budget, schedule, and personnel) to ensure that IA requirements are implemented, validated, and sustained. Ensuring quality controls are used during development and/or integration of software/applications is also the PM's responsibility.

Information Assurance Manger (IAM) and Information Assurance Officer (IAO)

The IAM is the individual responsible for the IA program of a DoD IS and/or organization. He or she consults with the PM on applicable IA policies and controls, ensuring that systems are developed within an acceptable level of risk. The IAM is often supported by an Information Assurance Officer (IAO), whom ensures the IAM's policies are implemented in day-to-day activities and tasks.

User Representative (UR)

The UR represents the interests of the user community, ensuring that user requirements are represented throughout the development and test of the system. URs must inform their DAAs on how the system is used in the field in support of the mission.

DIACAP ACTIVITIES AND ARTIFACTS

Unlike the DITSCAP's four phases, the DIACAP is organized into five activities. A comparison between the two processes is illustrated in Table 1.

Table 1. DIACAP Activities vs. DITSCAP Phases

DITSCAP Phases	DIACAP Activities
1 – Definition	1 – Initiate and Plan IA C&A
2 – Verification	2 – Implement and Validate Assigned IA Controls
3 – Validation	3 – Make Certification Determination and Accreditation Decision
4 – Post Accreditation	4 – Maintain ATO and Conduct Reviews
	5 – Decommission

In summary, the DIACAP adds a fifth activity, Decommission, which addresses the secure retirement of systems when they are removed from operation.

The DIACAP in its entirety, including its five activities, is explained in the following sections. Each activity section discusses the required artifacts to be delivered as a result of the activity. The artifacts of the DIACAP are new, contain more relevant information, are more streamlined, and are completely different from the main artifact of the DITSCAP, the System Security Authorization Agreement (SSAA). The DIACAP requires the completion of the following artifacts:

- System Identification Profile (SIP)
- DIACAP Implementation Plan (DIP)
- DIACAP Scorecard
- Plan of Action and Milestones (POA&M)
- Supporting documentation

These artifacts are described in their respective activities in which they are developed and/or updated.

Activity 1 – Initiate and Plan IA C&A

The goal of the first activity is to notify the appropriate stakeholders of the IS and the plan for its ensuing C&A effort. Four tasks are executed during this activity:

- Register the system
- Assemble the DIACAP team
- Assign IA controls
- Initiate DIACAP Implementation Plan (DIP)

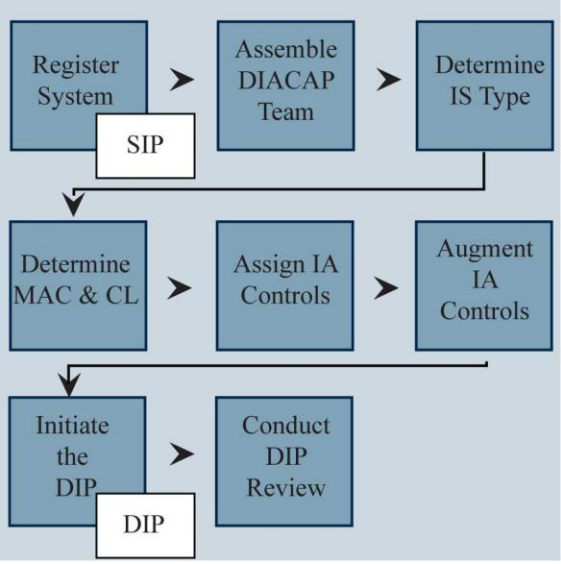

Figure 2. Activity 1 Workflow

Register the System
One of the first steps in any DIACAP effort is the registration of the system into the appropriate registration database. The registry ensures that the status of all ISs is visible to the DoD for tracking management and FISMA compliance reporting purposes, which is ultimately reported at the Congressional level.

Some organizations use their own internal registry; however, all of the registries report information into one centralized main registry, the DoD Information Technology Portfolio Registry (DITPR). Each system is registered based on the DoD Component and the appropriate GIG MA. The DITPR is a web-based system that provides information on applications and IT systems.

The set of information gathered during system registration is documented in an artifact called the System Identification Profile (SIP). The SIP is updated and maintained throughout the system's lifecycle. The SIP contains information that uniquely identifies the system, along with its accreditation status and system owner. The DIACAP Team is also identified within this document.

Assemble the DIACAP Team
The DIACAP Team includes those officials responsible for implementing the DIACAP on an IS. Each organization may have additional members for their DIACAP Team; however, the typical cast includes: the DAA, the SIAO/CA, the PM, the UR, and the IAM. Team members and their contact

information are documented in the SIP. Members of the team must have the requisite training and certifications in accordance with the Workforce Improvement Act [DoDD 8570.01-M]. Some positions may be held by the same person.

Assign IA Controls

Neither the task of assigning IA controls, nor the IA controls themselves have changed from DITSCAP to DIACAP. The controls in DoDI 8500.2, Enclosure 4, Attachments 1 through 6, are still being used. The main determining factors used in deciding which controls are applicable are also the same.

When assigning controls, the system owner must determine the IS type, which can be one of four options:

- Automated Information System (AIS)
- Enclave
- Outsourced IT-based Processes
- Platform IT Interconnection

After the IS type is determined, the Mission Assurance Category (MAC) and Confidentiality Level (CL) are determined. The selection of the applicable controls is determined by the MAC and CL combination as shown in Table 2.

Table 2. Controls Based on MAC and CL

MAC	CL	Controls - 8500.2 Attachments	Number of Controls
I	Classified	A1 and A4	110
I	Sensitive	A1 and A5	106
I	Public	A1 and A6	81
II	Classified	A2 and A4	110
II	Sensitive	A2 and A5	106
II	Public	A2 and A6	81
III	Classified	A3 and A4	105
III	Sensitive	A3 and A5	100
III	Public	A3 and A6	75

This baseline of controls is then augmented with any DoD component-level or system-level IA controls, such as DCID 6/3, AR 25-2, JAFAN 6/3, etc.

All of these controls are identified in an artifact called the DIACAP Implementation Plan (DIP), along with the implementation status of each assigned IA control. The DIP is a useful management tool for tracking the implementation of IA on systems. One major difference brought forth by the DIACAP is the notion of "inherited controls." An inherited IA control is an existing IA control and its C&A status that would extend from an "originating" system or site to another "receiving" system in order to model a real-world scenario of shared security infrastructure or capabilities. An example of inherited controls would be site-based controls, such as physical security and emergency services that a system would receive from the gaining site.

Initiate the DIP

In addition to the identification of assigned IA controls, the DIP also contains the strategy for implementing IA controls, implementation status, responsible entities, resources required, and estimated completion dates. The DIACAP Knowledge Service (KS) is an excellent resource for obtaining detailed information on descriptions, implementation, and expected test results for all IA controls.

Conduct the DIP Review

Prior to exiting Activity 1, a review of the DIP should be conducted. This ensures that the DIACAP team agrees on the assignment and planned implementation of IA controls. Once the DIP is approved by the DIACAP team, it is executed in Activity 2. The DIP is also a living document that is continuously updated throughout the lifecycle of the system. The DIP review should be conducted prior to the program's Critical Design Review as it contains the agreed upon IA requirements that are to be built into the system. Agreement from this review paves the way forward for the secure design of the IS and allows IA to be 'Baked-In' to the system as opposed to 'Bolted-On'.

Activity 2 – Implement and Validate Assigned IA Controls

The goals of Activity 2 include implementing the security controls into the information system and testing them to ensure their compliance. During this activity, residual risk is identified and documented along with the strategy and timeline for mitigating the risks. Four tasks shown in Figure 3 are executed to fulfill these goals:

- Execute the DIP
- Conduct validation activities
- Record compliance status
- Prepare IT security POA&M

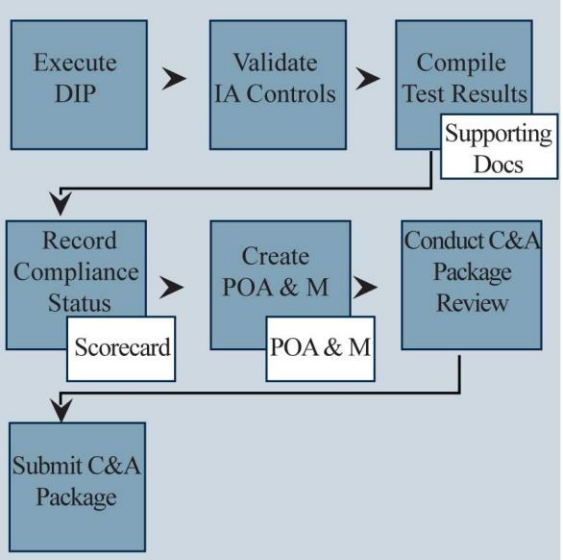

Figure 3. Activity 2 Workflow

Execute the DIP
The phrase, "Executing the DIP," summarizes all the behind the scenes coordination and integration between the system security engineers and all of the Integrated Product Teams to ensure that all of the assigned IA controls are implemented into the system in accordance with the implementation guidelines available on the DIACAP Knowledge Service website.

Validate Implementation of IA Controls
Controls are validated by an independent third-party using procedures that are maintained by the DIACAP Configuration Control and Management and posted on the DIACAP Knowledge Service. Each validation procedure describes preparation steps, validation steps, expected results, and criteria and protocols for recording results. During this time, the system is scanned for vulnerabilities using tools, such as eEye Retina®, DISA Gold Disk, Security Readiness Review Evaluation Scripts, and other approved tools. Any artifacts created as a result of the tests, such as screen shots and test tool reports, should be added as supporting documentation to the C&A package.

Other supporting information is also assessed at this time. Such information may include the Configuration Management Plan, Information Security Policy, Continuity of Operations Plan, and others as required.

Record Compliance Status
Once all of the data has been collected from the validation effort, it is analyzed and used to populate another DIACAP artifact referred to as the DIACAP Scorecard.

The DIACAP Scorecard is a summary report that discloses the system's validation results. Status of each assigned control is indicated with one of three abbreviations:

- Compliant "C" – IA Controls for which the expected results for all associated validation procedures have been achieved
- Non-compliant "NC" – IA Controls for which one or more of the expected results for all associated validation procedures are not achieved. Not achieving expected results for all validation procedures does not necessarily equate to unacceptable risk
- Not applicable "NA" – IA Controls that do not impact the IA posture of the IS as determined by the DAA and DIACAP Team

Prepare IT Security POA&M
The creation of the POA&M is a requirement passed down from the Office of Management and Budget. Its purpose is to identify and track tasks required to correct or mitigate weaknesses exposed during validation. Additionally, the document also lists the resources required to correct/mitigate the weakness, as well as, the responsible individual, scheduled completion dates, milestones, and statuses. The POA&M serves as a permanent record of all weaknesses of the system. When a weakness is corrected or mitigated, it is noted; however, the original weakness stays in the POA&M. Until all weaknesses are closed, the POA&M will continue to be monitored by the Component CIO.

Conduct DIACAP Comprehensive Package Review
It is recommended, not required, that the DIACAP team conduct a comprehensive package review to ensure completeness and accuracy of the DIACAP artifacts prior to the start of Activity 3. This review also ensures that no surprises exist in the package that is provided to the DAA.

Activity 3 – Make Certification Determination and Accreditation Decision

The goal of Activity 3 is to receive a favorable accreditation decision from the DAA. This activity is divided into two main tasks:

- Make certification determination
- Issue accreditation decision

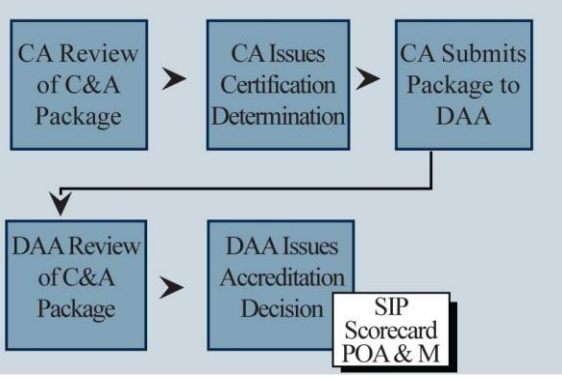

Figure 4. Activity 3 Workflow

Certification Determination
First, the CA reviews the entire C&A package. During this review, he or she assesses the overall reliability and viability of the DoD IS, the acceptability of the implementation and performance of IA safeguards, and the system's behavior in the larger information environment. The CA will look closely into all of the IA controls that were deemed non-compliant, their assigned impact and severity codes, the mitigation strategies employed, and the overall risk if the system is permitted to connect and/or operate.

Two codes assist in making this risk assessment: an impact code, which is an objective code assigned to each control to identify the level of impact associated with non-compliance of an IA control; and the severity code, which is a somewhat subjective code that is assigned based on the non-compliant control and other mitigating factors that may lessen its severity. Impact codes are expressed as High, Medium, and Low. The impact codes assigned to each control are determined by the DoD and cannot be altered. Impact codes are used in conjunction with severity codes to determine the urgency with which corrective action should be taken.

A severity code is assigned to each identified security weakness by the CA. Severity codes are expressed as:

- CAT I – The weakness must be corrected before an ATO is granted.
- CAT II – The weakness must be corrected or satisfactorily mitigated before an ATO can be granted.
- CAT III – The weakness will not prevent an ATO from being granted, if the DAA accepts the risk associated with the weakness.

The CA uses all of this information to make and issue a certification determination. A certification determination is required before an accreditation decision can be made.

Accreditation Decision
The accreditation decision is the official designation made by the DAA regarding his or her personal acceptance of risk associated with operating a particular information system. An accreditation decision is expressed as one of the following:

- Authorization to Operate (ATO) – An ATO grants the system full permission to operate as long as the system maintains its accredited IA posture. An ATO is valid for three years, unless a major change to the system requires the system to undergo re-certification and accreditation.
- Interim Authorization to Operate (IATO) – An IATO permits a system to operate while CAT II or CAT III weaknesses are undergoing correction or mitigation. An IATO must expire within 180 days. A DAA may not grant consecutive IATOs totaling more than 360 days. If a system fails to satisfactorily address weaknesses within the extended 360 days, it will receive a Denial of Authorization to Operate (DATO).
- Interim Authorization to Test (IATT) – An IATT is a special case accreditation decision that provides temporary permission for a system to operate in a live environment with live data for testing purposes. IATTs are reserved for systems that must be running live in order to fully test. The time allotted for an IATT is typically limited to a short timeframe and is tied to at least one test event.
- DATO – A DATO is issued when the DAA determines that the IS cannot operate due to inadequate IA design or failure to satisfactorily implement assigned IA controls. If a system is already operating when the DATO is issued, operation of the system is immediately ceased.

It is important to note that a DAA cannot assume the risk of any IS that has a weakness with a CAT I severity code finding. Thus, any system with a CAT I weakness will not be issued an ATO or an IATO.

The DAA's accreditation decision is represented in an updated Scorecard and a POA&M. The Scorecard contains both the CA's and DAA's signatures along with the dates of certification and accreditation. In

the POA&M, the DAA details the rationale of why he/she is willing to accept an IA control marked as NC. The SIP is also updated upon accreditation to indicate the C&A status and ATO period.

Activity 4 – Maintain Authorization to Operate and Conduct Reviews

Activity 4 is commenced once the IS receives an ATO. The goal of this activity is to maintain the IS's IA posture and maintain its operation within an acceptable level of risk. To achieve this goal, four tasks must be executed:

- Maintain situational awareness
- Maintain IA posture
- Conduct reviews
- Initiate reaccreditation

Figure 5. Activity 4 Workflow

Maintain Situational Awareness
Maintaining situational awareness is accomplished by monitoring the performance of the system and managing any potential vulnerabilities to the system. The PM must ensure that the IS's Information Assurance Vulnerability Management Plan (IAVMP) is being executed. The IAVMP details how IA Bulletins, Technical Tips, and Alerts are received and handled. The IAM may also conduct independent evaluations during this activity to ensure that the IS is still operating as expected.

Maintain IA Posture
The IS must maintain its IA posture as accredited to ensure continuation of its ATO and to avoid receiving a DATO. Anytime during operation and sustainment of the system, the IAM may assign additional IA controls or call for modifications in the design of the IS. In order to prevent a DATO, the system will need to implement these recommendations.

Conduct Reviews
In order to comply with FISMA mandates, the IAM must ensure that annual reviews and testing are performed and that results are reported. The IAM provides the results of the annual reviews to the DAA and CA by the corresponding due date listed in the SIP. The annual reviews/tests that are required under FISMA include:

- Annual Security Review and Security Control Test – This requirement ensures assigned IA controls are reviewed/tested. The PM must provide a written statement to the CA that confirms the effectiveness of the assigned IA Controls and their implementation. The statement may also include recommended changes or improvements to the implementation of the IA controls, the assignment of additional IA controls, or design improvements to the overall system.
- System Contingency Plan Test – The PM is responsible for developing a baseline contingency plan for inclusion into the C&A Package. The testing of the contingency plan must be performed annually.

Initiate Reaccreditation
Any IS must undergo reaccreditation at least once every three years. Reaccreditation may occur earlier if the system's configuration is modified or it is deemed necessary given the results of one of the annual reviews. The annual requirements can be conducted by the PM, however every third year, the assessment and reaccreditation must be conducted by a third-party independent evaluator.

Activity 5 – Decommission

When a DoD IS is removed from operation, a number of IA-related events are initiated. Any IS that inherited controls from the decommissioned system must be evaluated for impact. The SIP must be updated to reflect the status of the system and other DIACAP-related artifacts should be removed from all tracking systems. Other data and objects, such as key management, identity management, vulnerability management, and privilege management should be evaluated for impact. Lastly, all supporting documentation should be disposed of in accordance with sensitivity/classification level.

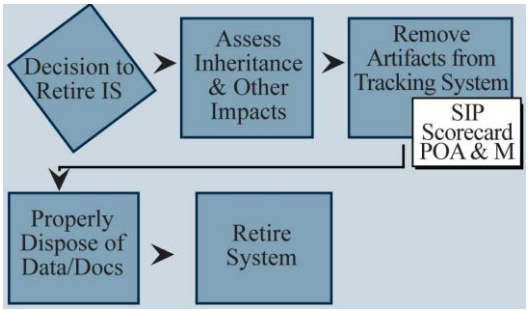

Figure 6. Activity 5 Workflow

DITSCAP vs. DIACAP ARTIFACT SUMMARY

The artifacts used for the DITSCAP versus the DIACAP are completely different, though some were previously portions of the SSAA. The DIACAP is a more streamlined process that requires less documentation, resulting in the reduction of potentially hundreds of pages formerly found in the SSAA. The decision on what is required is made by the DIACAP team and ultimately the DAA. At a minimum, the SIP, DIP, Scorecard, and POA&M will be required; additional Supporting Documents (SD) will be identified by the DIACAP team. Table 3 lists how the sections and appendices of the DITSCAP SSAA map to the artifacts of the DIACAP.

Table 3. DITSCAP SSAA to DIACAP Artifacts

DITSCAP		DIACAP
Sect 1	Mission Description	SIP/DIP
	User Description/Clearances	SD
Sect 2	Operating Environment	SD
	Physical Security Measures	SD
	Threat Analysis	POA&M
	Security Roles	SD
Sect 3	System Architecture	SD
	Accreditation Boundary	DIP
	External Interfaces/Dataflow	SD
	Hardware List	DIP
	Software List	DIP
	Ports, Protocols, and Services	DIP
Sect 4	System Security Requirements	SIP
Sect 5	Organization and Resources	SIP
Sect 6	Certification Level of Effort	N/A
	C&A Tasks and Milestones	DIP
App A	Acronyms	N/A
App B	Definitions	N/A
App C	References	N/A
App D	CONOPS	SD
App E	ISSP	SD
App F	SRTM	DIP
App G	CT&E	DIP
App H	ST&E	DIP
App I	Artifacts	SD
App J	System Rules of Behavior	SD
App K	Incident Response Plan	SD
App L	Contingency Plan	SD
App M	Personnel & Tech Security Cntrls	SD
App N	MOA/MOU	SD
App O	SETA	SD
App P	Test Results	POA&M
App Q	Risk Assessment	Scorecard
App R	Certification Statements	SD

FUTURE OF INFORMATION ASSURANCE

Rumors of yet another IA evolution have already surfaced. As a result of the C&A Transformation Initiative, led by the Associate Director of National Intelligence and Chief Information Officer (ADNI&CIO), the Assistant Secretary of Defense for Networks and Information Integration and DoD Chief Information Officer (ASD (NII)/DoD CIO), and the National Institute of Standards and Technology (NIST) a new draft NSS Instruction No. 1253 entitled, "Security Control Catalog for National Security Systems" was released.

The C&A Transformation Initiative addresses five goals:

- Define a common set of (trust) impact levels and eliminate the use of many different levels with different names based on different impact criteria (Ex: Protection Levels vs. MAC and CL)
- Create a federated framework where approval decisions made by different organizations are accepted across the board
- Define a comprehensive set of common security controls
- Elevate visibility and responsibility to a senior executive level to allow for more informed, consistent decisions with the entire "enterprise" in mind
- Create a common process that is adaptable to various development environments

Analysts are still not 100% clear on whether the new C&A process and Security Control Catalog (SCC) will be required for only those systems classified as, or connecting to National Security Systems (NSS), or if it will be adopted/mandated across all Federal Systems. The transition for rolling out the new instruction is happening today with initial use of the instruction expected late 2008/early 2009 (government fiscal year).

Overview of the Draft Risk Management Framework

The draft process, called the "Risk Management Framework," is broken up into eight activities and leverages draft security standards and guidance documents associated with each activity. The activities include:

- Categorize the IS
- Select security controls
- Supplement security controls

- Document security controls
- Implement security controls
- Assess security controls
- Authorize the IS
- Monitor the IS

Categorizing the IS is similar to the DIACAP's determination of the IS's MAC and CL level. During this activity, the Security Category (SC) of the system is determined. The SC is broken up into three major factors, including the impact of compromise of confidentiality, integrity, and availability. The impact is measured as Low-impact, Moderate-impact, and High-impact. The impact levels for each factor are then used in the selection of security controls.

The new Security Control Catalog contains 179 controls with 352 total control enhancements. This is in comparison to 8500.2's 110 controls. The basic control contains a control statement of the specific security capability required to protect that aspect of the IS. Control enhancements include additional functionality added to the basic control that increases the strength of the basic control.

The artifacts supporting this process will include a System Security Plan (SSP), a Security Assessment Report, and a POA&M. Reduction in documentation is one of the objectives of the new process and will be facilitated by leveraging automated tools when possible.

More information on the new national C&A Transformation will continue to surface as the transition continues. By December 2008, much more information should be available, and the path forward should provide more clarity.

CONCLUSION

The Information Assurance concept has evolved over the past 60 years, and the end is not in sight. The welcomed replacement of the DITSCAP with the DIACAP has led to a more streamlined process with greater visibility and responsibility to higher levels, ensuring that IA is managed consistently across the larger enterprise. As we work to adjust to the new DIACAP, rumors of a new process are already surfacing. It is largely possible that another year will bring forth the need to learn yet another process for performing IA. However, the changes in process steps and artifact formats have not blurred the overall purpose of IA, which is implementing the requisite security controls to ensure the security of our information, systems, and our country's national security so that we can continue to learn, train, and win!

ACKNOWLEDGEMENTS

We would like to thank all the individuals that played some role in the development of this paper. All conversations, reviews, editing efforts, and feedback in regards to this paper contributed to the final product.

REFERENCES

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

Department of Defense, (2007). *8510.01 Department of Defense (DoD) Information Assurance Certification and Accreditation (C&A) Process (DIACAP) Guidance.*

Department of Defense, (2005). *8570.1-M Information Assurance Workforce Improvement Program.*

Ehlers, Sharon, (December 13, 2007). *Certification and Accreditation Transformation Overview*. Retrieved April 27, 2008 from http://www.acsac.org/2007/casestudies/Ehlers.pdf

Office of the Director of National Intelligence/Chief Information Officer, (2007). *NSS Instruction No. 1253 Security control Catalog for National Security Systems.*

Program Executive Office for Simulation, Training and Instrumentation (PEO STRI), (2008). *Basic Accreditation Manual (BAM).*

Wierum, Jenifer M. (March 2005). *Defense Information Assurance Certification and Accreditation Process (DIACAP) and the Global Information Grid (GIG) Information Assurance (IA) Architecture*. Retrieved April 27, 2007 from http://www.afei.org/documents/DIACAPandtheGIGCCRTS_371.pdf