Deloitte.

Understanding the Department of Defense Information Assurance Certification & Accreditation Process

Leila Armogan

Contents

1.0 Introduction

The Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) is a Department of Defense (DoD) process used to ensure that risk management is applied to DoD information systems.The objective of the DIACAP is to obtain formal certification and accreditation (C&A) of a DoD system.

The DIACAP must be initiated and certification obtained for all DoD owned or controlled systems that receive, process, store, and display or transmit DoD information throughout the entire life cycle, regardless of classification or sensitivity of the information or information system.[1] The DIACAP is an important aspect of managing the Information Assurance (IA) posture of a DoD system and is used to certify systems for compliance with DoD security requirements and obtain Authority To Operate (ATO) by a Designated Accrediting Authority (DAA).

ATO is a formal decision made by the DAA that authorizes the operation of a system and certifies that the system meets all operational requirements. All DoD systems require an ATO before they become fully operational. To obtain an ATO, IA professionals must execute a DIACAP. DoD systems with an ATO must be reviewed annually to maintain the ATO by confirming that the IA posture of the system remains acceptable.[2]

In accordance with OMB Circular A-130, a system must be recertified and reaccredited once every 3 years. A new DIACAP must be initiated when the system ATO approaches its recertification date. In addition, the results of an annual review or a major change in system IA posture may also indicate the need for recertification and reaccreditation of a system. Examples of major changes in IA posture include a change in system location or major changes to system code.

This whitepaper provides an overview of the five activities included in the DIACAP process, identifies the roles and responsibilities of key stakeholders involved in the DIACAP for a DoD system, and identifies ATO best practices. The ATO best practices are applicable when an existing system with an ATO approaches its reauthorization date, when a major change in system IA posture occurs, or when the results of an annual review indicate the need for recertification and reaccreditation. Regardless of the specific reason for initiating the DIACAP to maintain ATO, an ATO package must be submitted to the DAA for approval. The ATO best practices in this whitepaper are therefore a helpful resource for those preparing an ATO package for the DAA.

1.1 Overview of DIACAP Compliance Activities[3]

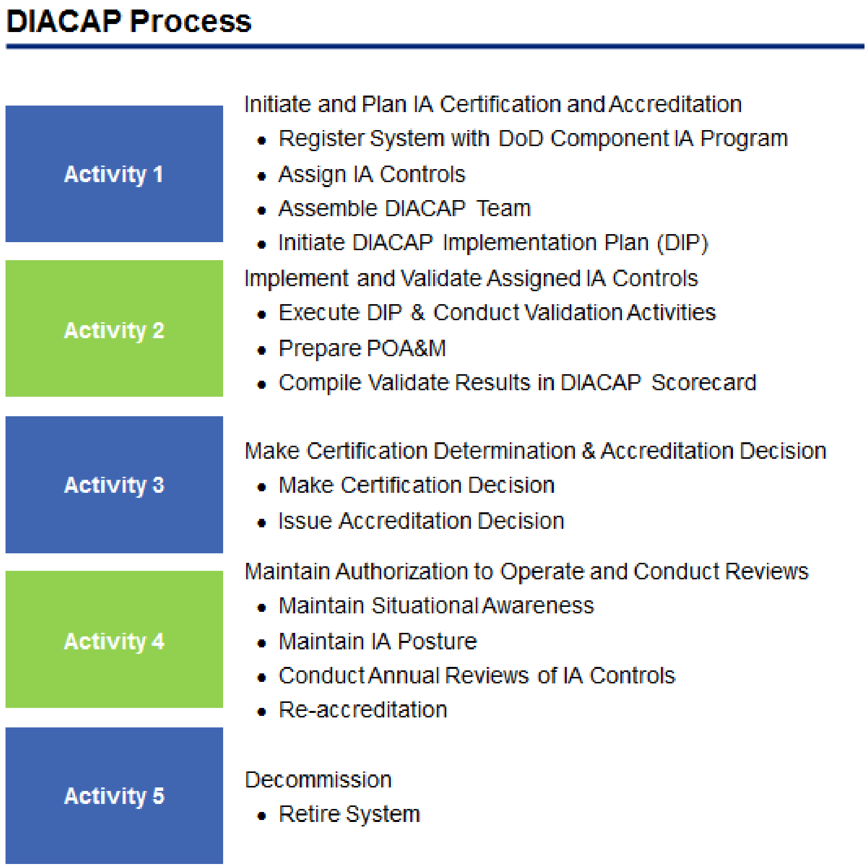
As depicted in Figure 1: DIACAP Process, there are five primary activities that are necessary to become DIACAP compliant. The descriptions of each activity in Figure 1: DIACAP Process are described in further detail in sections 1.1.1 – 1.1.5 and are sourced from Department of Defense Instruction (DODI) 8510.01, which

[1] CIO Support Department of Defense Information Assurance Certification and Accreditation Program (DIACAP), From Personnel and Readiness Information Management (P&R IM): http://www.prim.osd.mil/cap/dhra-diacap.html?p=1.1.1.1.1

[2] Got DIACAP? Slick Sheet, From Personnel and Readiness Information Management (P&R IM): http://www.prim.osd.mil/cap/dhra-diacap.html?p=1.1.1.1.1

[3] Department of Defense Instruction (DODI) 8510.01. "DoD Information Assurance Certification and Accreditation Process (DIACAP)" November 28, 2007: http://www.dtic.mil/whs/directives/corres/pdf/851001p.pdf

contains the final version of the DIACAP. For additional information on any of the DIACAP activities, refer to DODI 8510.01.



DIACAP Process

Activity 1

Initiate and Plan IA Certification and Accreditation

- Register System with DoD Component IA Program
- Assign IA Controls
- Assemble DIACAP Team
- Initiate DIACAP Implementation Plan (DIP)

Activity 2

Implement and Validate Assigned IA Controls

- Execute DIP & Conduct Validation Activities
- Prepare POA&M
- Compile Validate Results in DIACAP Scorecard

Activity 3

Make Certification Determination & Accreditation Decision

- Make Certification Decision
- Issue Accreditation Decision

Activity 4

Maintain Authorization to Operate and Conduct Reviews

- Maintain Situational Awareness
- Maintain IA Posture
- Conduct Annual Reviews of IA Controls
- Re-accreditation

Activity 5

Decommission

- Retire System

Figure 1: DIACAP Process

1.1.1 Activity 1 – Initiate and Plan IA Certification & Accreditation

This activity includes registering the system with the governing DoD Component IA program (refer to the DIACAP Knowledge Service for specific registration instructions), assigning IA controls based on Mission Assurance Category (MAC) and Confidentiality Level (CL), identifying the DIACAP Team for the system (refer to section 1.2 for additional information), and initiating the system's DIACAP Implementation Plan (DIP).

Definitions of key terms associated with Activity 1 are provided below:

- **DIACAP Knowledge Service**: A web-based resource developed by the DoD that functions as a widely recognized source for DIACAP policy and guidance. The DIACAP Knowledge Service is a resource for fulfilling the requirements of the DIACAP and contains tools, documentation, IA controls, and IA control implementation and validation procedures. Access to the DIACAP Knowledge Service requires a DoD Public Key Infrastructure (PKI) certificate or an External Certification Authority (ECA) PKI certificate.

- **IA Controls**: Used to establish IA requirements for DoD systems. Pre-defined IA controls (known as baseline IA controls) are based on the MAC and CL associated with a system. There are 3 DoD MAC levels and 3 DoD CL levels. Each MAC or CL represents increasingly rigorous IA requirements. For information about how a system's assigned MAC and CL determine a system's baseline IA controls, refer to DoD Instruction 8500.2, Enclosure 4, "Baseline Information Assurance Levels."

- **Mission Assurance Category (MAC) Levels**: Each DoD system is assigned a MAC level. DoD Instruction (DODI) 8580.1 "Information Assurance in the Defense Acquisition System" defines the 3 MAC levels as follows:

    - **MAC I systems**: Handle information vital to the operational readiness of deployed or contingency forces. Since the loss of MAC I data would cause severe damage to the successful completion of a DoD mission, MAC I systems must maintain the highest levels of both integrity and availability and use the most rigorous measure of protection.

    - **MAC II systems**: Handle information important to the support of deployed and contingency forces. The loss of MAC II systems could have a significant negative impact on the success of the mission or operational readiness. The loss of availability of MAC II data can be tolerated only for a short period of time, so MAC II systems must maintain a medium level of availability. MAC II systems require protective measures above industry best practices to ensure adequate integrity and availability of data.

    - **MAC III systems**: Handle information necessary for day-to-day operations, but not directly related to the support of deployed or contingency forces. The loss of MAC III data would not have an immediate impact on the effectiveness of a mission or operational readiness. MAC III systems are required to maintain basic levels of integrity and availability. MAC III systems must be protected by measures considered as industry best practices.[4]

- **Confidentiality Levels (CLs)**: Each DoD system is assigned a CL that is based on the sensitivity of information associated with the system. Department of Defense Directive 8500.01E "Information Assurance[5]" defines the 3 CLs as follows:

    - **Classified**: Systems that process classified information.

    - **Sensitive**: Systems that process sensitive information.

    - **Public**: Systems processing publicly releasable information.

- **DIACAP Implementation Plan (DIP)**: Identifies a system's IA controls, including inherited IA controls, which are shared by at least two systems. The DIP also includes IA control implementation status, responsible resources, and the estimated completion date for each IA control.

[4] DoD Instruction (DODI) 8580.1. "Information Assurance in the Defense Acquisition System." July 9, 2004: http://www.dtic.mil/whs/directives/corres/pdf/858001p.pdf

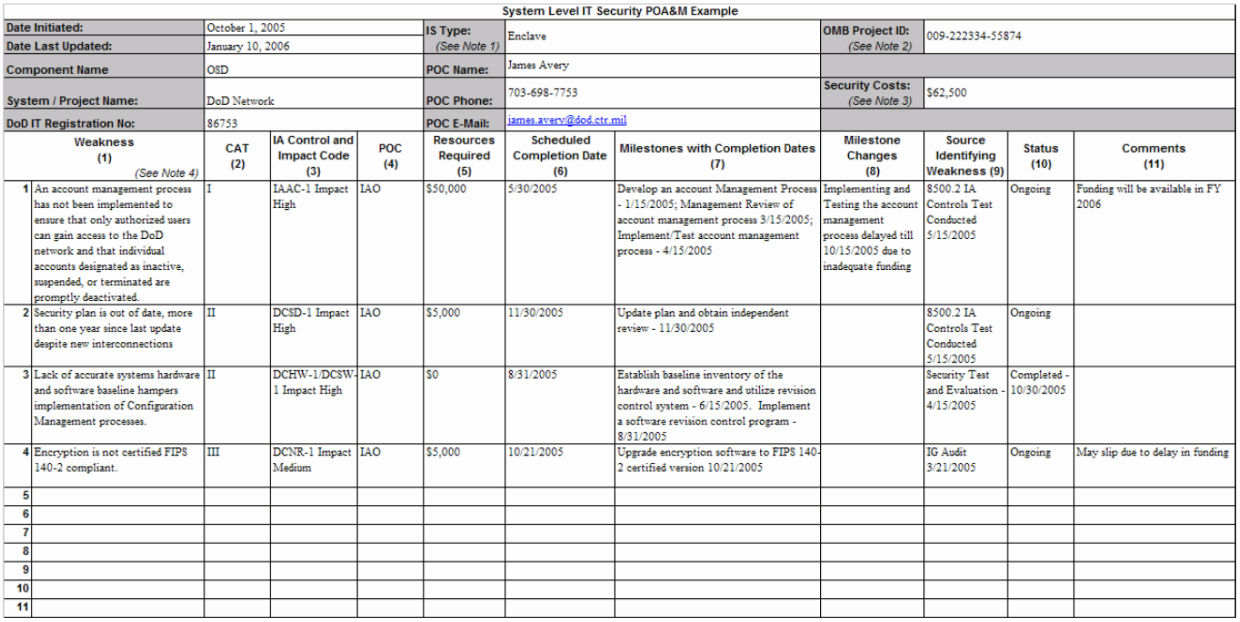
[5] Department of Defense Directive 8500.01E. "Information Assurance." Certified Current as of April 23, 2007: http://www.dtic.mil/whs/directives/corres/pdf/850001p.pdf

1.1.2 Activity 2 − Implement and Validate Assigned IA Controls

This activity involves implementing the DIP, conducting validation activities (refer to the DIACAP Knowledge Service for additional information), preparing the Plan of Action & Milestones (POA&M), and compiling validation results (i.e. the status of each IA control).

- **DIP**: For a description of the DIP, refer to 1.1.1 Activity 1 − Initiate and Plan IA Certification & Accreditation.

- **POA&M**: Documents and tracks the status of any corrective actions associated with a certification and accreditation decision. Figure 2: Sample POA&M is a sample POA&M from DoD Instruction 8510.01, "DoD Information Assurance Certification and Accreditation Process (DIACAP) that shows the necessary information that must be captured in a POA&M.



System Level IT Security POA&M Example

Date Initiated:	October 1, 2005	IS Type: (See Note 1)	Enclave	OMB Project ID: (See Note 2)	009-222334-55874
Date Last Updated:	January 10, 2006				
Component Name	OSD	POC Name:	James Avery		
System / Project Name:	DoD Network	POC Phone:	703-698-7753	Security Costs: (See Note 3)	$62,500
DoD IT Registration No:	86753	POC E-Mail:	james.avery@dod.ctr.mil		

	Weakness (1) (See Note 4)	CAT (2)	IA Control and Impact Code (3)	POC (4)	Resources Required (5)	Scheduled Completion Date (6)	Milestones with Completion Dates (7)	Milestone Changes (8)	Source Identifying Weakness (9)	Status (10)	Comments (11)
1	An account management process has not been implemented to ensure that only authorized users can gain access to the DoD network and that individual accounts designated as inactive, suspended, or terminated are promptly deactivated.	I	IAAC-1 Impact High	IAO	$50,000	5/30/2005	Develop an account Management Process - 1/15/2005; Management Review of account management process 3/15/2005; Implement/Test account management process - 4/15/2005	Implementing and Testing the account management process delayed till 10/15/2005 due to inadequate funding	8500.2 IA Controls Test Conducted 5/15/2005	Ongoing	Funding will be available in FY 2006
2	Security plan is out of date, more than one year since last update despite new interconnections	II	DCSD-1 Impact High	IAO	$5,000	11/30/2005	Update plan and obtain independent review - 11/30/2005		8500.2 IA Controls Test Conducted 5/15/2005	Ongoing	
3	Lack of accurate systems hardware and software baseline hampers implementation of Configuration Management processes.	II	DCHW-1/DCSW-1 Impact High	IAO	$0	8/31/2005	Establish baseline inventory of the hardware and software and utilize revision control system - 6/15/2005. Implement a software revision control program - 8/31/2005		Security Test and Evaluation - 4/15/2005	Completed - 10/30/2005	
4	Encryption is not certified FIPS 140-2 compliant.	III	DCNR-1 Impact Medium	IAO	$5,000	10/21/2005	Upgrade encryption software to FIPS 140-2 certified version 10/21/2005		IG Audit 3/21/2005	Ongoing	May slip due to delay in funding
5											
6											
7											
8											
9											
10											
11											

Figure 2: Sample POA&M

1.1.3 Activity 3 − Make Certification Determination and Accreditation Decision

The Certifying Authority (CA) makes the certification decision based on the overall assessment of the DoD system. The certification decision considers impacts associated with IA controls in a non-compliant status, associated severity categories, and cost to correct or mitigate. The weaknesses identified on the POA&M reflect risk to the system.

The CA assigns one of the following severity categories to system weaknesses. Every CAT I, CAT II, and CAT III weakness must appear on the POA&M until resolved.

- **CAT me**: Weaknesses must be corrected before an ATO is granted.

- **CAT II**: Weaknesses must be corrected or mitigated before an ATO is granted. The CAT II weakness must be corrected or mitigated within 180 days of the accreditation decision.

- **CAT III**: Weaknesses do not prevent an ATO from being granted if the DAA accepts the risk associated with the weaknesses.

A certification decision is required before an accreditation decision can be made. The DAA issues one of the following accreditation decisions. If requested by the DAA, documentation supporting an accreditation decision is provided electronically.

- **Authority to Operate (ATO)**: A DoD system that has obtained authorization to process, store, or transmit information. An ATO indicates a DoD system adequately implemented all assigned IA controls. An ATO accreditation decision must specify an authorization termination date, which specifies when the ATO expires. The termination date must be within three years of the authorization date.

- **Interim ATO (IATO)**: A DoD system that has obtained temporary authorization to operate under the conditions or constraints identified in the accreditation decision. The IATO accreditation decision must specify and authorization to terminate date within 180 days of the authorization date. The DAA cannot grant consecutive IATOs totaling more than 360 days.

- **Interim Authorization to Test (IATT)**: A temporary authorization to test a DoD system in a specific operational environment or with live data for a specified time period.

- **Denial of ATO (DATO)**: A DoD system cannot operate due to inadequate IA design, failure to adequately implement assigned IA controls, or other lack of adequate security. IATTs are granted only when live data is required to complete specific test objectives (e.g., replicating certain operating conditions in the test environment is impractical).

1.1.4 Activity 4 − Maintain ATO and Conduct Reviews

Maintaining ATO is contingent on the sustainment of acceptable IA posture. The Information Assurance Manager (IAM) has primary responsibility for maintaining situational awareness and initiating actions to improve or restore IA posture. The IAM continuously monitors the system for security-relevant events and configuration changes that negatively impact IA posture and periodically assesses the quality of IA control implementation. In addition, the IAM may schedule a revalidation of any or all IA controls at any time based on an independent decision or at the direction of the CA or DAA.

In accordance with OMB Circular A-130, a system must be recertified and reaccredited once every 3 years. The results of an annual review or a major change in the IA posture at any time may also indicate the need for recertification and reaccreditation of the system. DoD systems with a current ATO that are found to be operating in an unacceptable IA posture will have any newly identified weakness added to an existing or newly created POA&M.

1.1.5 Activity 5 − Decommission

Prior to decommissioning a system, any inheritance relationships are reviewed and assessed for impact. Once the system is decommissioned, the POA&M should be removed from the tracking system and supporting documentation disposed of based on sensitivity or classification level.

2.0 DIACAP Team

The roles and responsibilities of members of the DIACAP Team are included in this section. The roles identified in this section are necessary for implementing a DIACAP for a DoD system.

2.1 Program Manager

As documented in DoDI 8510.01[6], the Program Manager is responsible for the following:

- Ensuring that each DoD system has a designated IAM.
- Implementing the DIACAP for assigned DoD systems.
- Planning and budgeting for IA control implementation, validation, and sustainment throughout the system life cycle.
- Ensuring that system security engineering is employed to implement or modify the IA component of the system architecture.
- Enforcing DAA accreditation decisions for hosted or interconnected DoD systems.
- Developing, tracking, resolving, and maintaining the DIP for DoD systems.
- Ensuring POA&M development, tracking, and resolution.
- Making sure that system annual reviews are conducted as required by the Federal Information Security Management Act of 2002 (FISMA).

2.2 Designated Accrediting Authority

As documented in DODI 8510.01[7] and DoDI 8500.2[8], the DAA is responsible for the following:

- Ensuring a DIACAP package is initiated and completed for assigned DoD systems.
- Making sure all assigned DoD systems comply with applicable DoD baseline Information Assurance (IA) controls.
- Issuing accreditation decisions (i.e. authorizing or denying the operation of a DoD system). Accreditation decisions are expressed as an ATO, IATO, IATT, or a DATO.
- Assigning all IA-related positions in writing and including a statement of IA responsibilities.

[6] Department of Defense Instruction (DODI) 8510.01. "DoD Information Assurance Certification and Accreditation Process (DIACAP)" November 28, 2007: http://www.dtic.mil/whs/directives/corres/pdf/851001p.pdf

[7] Department of Defense Instruction (DODI) 8510.01. "DoD Information Assurance Certification and Accreditation Process (DIACAP)" November 28, 2007: http://www.dtic.mil/whs/directives/corres/pdf/851001p.pdf

[8] DODI 8500.2. "Information Assurance (IA) Implementation." February 6, 2003: https://acc.dau.mil/adl/en-US/378014/file/51140/ref%20e_DODI850002p_Info%20Assure%20Implementation.pdf

- Ensuring appointees to DIACAP positions receive appropriate IA training.
- Incorporating IA as an element of DoD information system life-cycle management processes.
- Ensuring all IAMs are U.S. citizens.
- Granting DoD systems formal accreditation to operate according to DoD IA certification and accreditation.

2.3 Information Assurance Manager

As documented in DODI 8510.01[9] and DoDI 8500.2[10], the IAM is responsible for the following:

- Supporting the PM in implementing the DIACAP.
- Advising and informing the governing IA program on DoD system C&A status and issues.
- Complying with the governing DoD IA program information and process requirements, including initiating actions to improve or restore IA posture.
- Recommending changes or improvement to the implementation of assigned IA controls, assigning additional IA controls, or changing or improving the design of the system itself.
- Providing an annual written statement to the DAA and the CA to report on the results of the IA control review. The written statement confirms the effectiveness of assigned IA controls, recommends changes in accreditation status, or recommends the development of a POA&M.
- Establishing information ownership responsibilities for each DoD information system including accountability, access approvals, and special handling requirements.
- Ensuring that IAOs are appointed in writing.
- Developing an IA program that identifies IA personnel and IA processes and procedures.
- Providing oversight to the IAO to ensure established IA policies and procedures are followed.
- Developing and maintaining IA certification documentation.
- Maintaining a repository for all IA certification and accreditation documentation.

[9] Department of Defense Instruction (DODI) 8510.01. "DoD Information Assurance Certification and Accreditation Process (DIACAP)" November 28, 2007: http://www.dtic.mil/whs/directives/corres/pdf/851001p.pdf

[10] DODI 8500.2. "Information Assurance (IA) Implementation." February 6, 2003: https://acc.dau.mil/adl/en-US/378014/file/51140/ref%20e_DODI850002p_Info%20Assure%20Implementation.pdf

- Ensuring that all IAOs receive the necessary technical and IA training, education, and certification to carry out their IA duties.
- Making sure that compliance monitoring occurs.
- Reviewing the results of compliance monitoring.
- Ensuring that IA inspections, tests, and reviews are coordinated.
- Ensure that all IA management review items are tracked and reported.
- Reporting incidents to the DAA and the DoD and coordinating responses to IA-related alerts.
- Acting as the primary IA technical advisor to the DAA.
- Notifying the DAA of any changes impacting the IA posture of an assigned DoD system.

2.4 Information Assurance Officer

The IAO is responsible for the following:

- Implementing user-focused policies and standard operating procedures (SOPs).
- Establishing and enforcing system contingency, continuity, and emergency plans.
- Monitoring and reporting unusual system activities.
- Implementing password maintenance and administration.
- Implementing rule and role-based access control.
- Implementing and enforcing information system security policies and practices in accordance with federal laws, national standards, and organizational policies and procedures.
- Integrating and implementing encryption standards.
- Implementing physical access control methods and procedures and defining system access control requirements.
- Establishing access restrictions that facilitate physical, technical, and administrative control measures including defining organizational requirements specific to the Defense in Depth philosophy.
- Implementing methods and control procedures that ensure the secure and proper disposition of hardware, software, memory components, and recordable information storage media.
- Implementing proper methods for declassifying or destroying hardware, software, and memory components used to process sensitive, classified, or national intelligence data.
- Ensuring the effective implementation of configuration controls including requirements to control changes to the trusted hardware and software baseline.

- Performing backup procedures and system restoration and recovery processes for critical information infrastructures.

- Identifying, analyzing, and evaluating system threats and vulnerabilities and their impact on the organization's critical information infrastructure.

- Assisting the IAM in meeting all responsibilities identified in section 2.3, Information Assurance Manager.

2.5 Certifying Authority

The CA is responsible for the following:

- Making certification decisions, which indicate the degree to which a system complies with assigned IA controls. The CA's certification decision identifies and assesses the residual risk with operating a system and the costs to correct or mitigate IA security weaknesses as documented in the POA&M.

- Reviewing the annual statement from the IAM that reports on the results of the annual IA control review and determining the necessary course of action.

3.0 Best Practices for Preparing ATO Package

The ATO best practices identified within this section are a helpful resource for those preparing an ATO package for the DAA.

3.1 Perform Monthly Asset Scanning and Reporting

Use an effective and timely automated tool (i.e. Retina, App Detective, Web Inspect, Gold Disk) to perform monthly assessments of system assets. Use the results of these monthly assessments to analyze the system for accuracy, completeness, and IA compliance. Track all system shortcomings to resolution using a POA&M, which will ensure that system shortcomings are resolved in a timely manner. Provide the results of the monthly assessments to the IAM and retain the results for future reference.

3.2 Recognize Differences in Accrediting Stationary vs. Remote Systems

Ensure that the CS Team and the IA Team understand the differences between accrediting stationary systems (i.e. with a physical site) vs. remote systems (i.e. with no physical site). Policies and procedures are in place for accrediting stationary systems, but there are no policies and procedures in place for accrediting remote systems. If accrediting a remote system, meetings should be held between the IA Team and the CS Director to address and better understand the accreditation process for remote systems.

3.3 Ensure Use of Correct CS Templates

The CS Team releases new system deliverable templates on a regular basis. The most up-to-date templates are to be used whenever an ATO package is submitted to the DAA for approval. Before beginning work on the system deliverable documentation included in the ATO package, obtain the most recent CS templates from the CS Team. The templates available from the CS Team include the following:

- DIACAP Implementation Plan
- System Policy
- System Security Plan

- Annual IA Review Plan
- Rules of Engagement
- Rules of Behavior
- Business Impact Analysis
- Contingency Plan
- Continuity of Operations (COOP)
- Incident Response Plan, Information Assurance Training Plan
- Quality Assurance Plan
- Security Design Document
- Audit Policy, Configuration Management Plan
- Information Assurance Vulnerability Management Plan
- System Administrator Guide

3.4 Ensure Effective Communication Between IAO and Technical Staff

In order to accomplish the goal of maintaining a system's compliance posture, effective communication needs to occur between the IAO and the technical staff for the system. Effective communication will help to ensure that activities and artifacts associated with system compliance posture is undertaken in a timely manner and attention to detail is applied. In addition, communication regarding effective management tools and planning strategies must be put in anticipation of upcoming events.

3.5 Clarify Roles and Responsibilities

Ensure that roles and responsibilities related to the completion of system documentation deliverables are clearly defined prior to starting work on the ATO package. Identifying who is responsible for each system documentation deliverable prior to starting work on the ATO package will prevent unnecessary delays.

3.6 Use Detailed Communication Instead of High Level

Make sure all communication is clearly understood between the IA Team and those preparing the system documentation deliverables for the ATO package. For example: In situations where the IA team returns system documentation deliverables for corrections, those responsible for preparing the documentation deliverables should clarify with the IA team the specific format in which comments are to be addressed within the documentation deliverables. Any uncertainty regarding the meaning of an IA Team comment should also be clarified. Without very clear and precise communication, the amount of time needed to complete and approve the system documentation deliverables will greatly increase. This is due to re-work on the system documentation deliverables resulting from unclear communication.

3.7 Start System Documentation Deliverables Well in Advance of ATO

Start the updates to the system documentation deliverables for inclusion in an ATO Package at least 6 months prior to the submission due date to the DAA. This will provide the needed time to review the existing documentation, assess the extent of the necessary changes, and incorporate the necessary changes.

3.8 Ensure Top Level Documents are Complete Prior to Submitting ATO Package

The Service Level Agreement (SLA), Memorandum of Agreement (MOA), and Interconnection Service Agreement (ISA) should be complete before starting work on the ATO deliverables and submitting the ATO package to the DAA. The CS Team will request these documents.

3.9 Review the POA&M Guide Prior to Working on the POA&M

The POA&M Guide provides much needed guidance for those working on the POA&M. Reviewing the POA&M Guide is especially important for those with little to no prior POA&M experience.

3.10Provide Sufficient Evidence for False Positives

For POA&M findings deemed false positives, steps must be taken to prove that the finding is in fact a false positive. This is most commonly accomplished via a screenshot or in-person observation. Screenshots or documentation about findings that were accepted as false positives during an in-person walk through are key to ensuring concurrence by the CS Team. Coordination with varying stakeholders is often necessary to obtain the necessary screenshots and supporting documentation.

3.11Associate Each POA&M Item with Responsible Party

For each POA&M item, associate a responsible party. Without a contact associated with each POA&M item, there is often confusion as to who to follow-up with. Assigning a contact to each POA&M item results in quicker resolution of POA&M questions and concerns.

3.12Automate Assessments and Artifact Reviews

Ensure annual reviews of system documentation to verify accuracy, relevance, and completeness of documentation and to incorporate necessary updates to system documentation. Apply any new artifact templates released by the CS team during these annual reviews.

3.13Ensure Sufficient Staffing of Maintenance Support Personnel

Make sure maintenance support is fully staffed to provide the proper security requirements under the ATO and document the maintenance support requirements in the SLA. The SLA is to identify the complete solution to support the required end state ATO requirements.

3.14Identify Site Recovery Support Requirements

Identify the site-level Point-of-Contacts (POCs) to support requirements for continuity of operations (COOP) and disaster recovery. In the event that funding is not secure for this activity, having these individuals identified will allow for the requirements once funding becomes available.

4.0 Conclusion

Ensuring that a DoD system obtains certification and accreditation through the implementation of the DIACAP ensures that risk management is applied to a DoD system. DoD Instruction 8510.01 and DoD Instruction 8500.2 are authoritative sources of information on the DIACAP and are the primary sources of the content in this whitepaper. For additional information on the DIACAP, refer to the following resources:

- **DIACAP Knowledge Service** – Contains A DoD authoritative source for DIACAP policy and guidance: https://diacap.iaportal.navy.mil/login.htm

- **Defense Information Systems Agency (DISA) Online DIACAP Training −** http://iase.disa.mil/diacap/

- **DISA Online Awareness Training:** Provides a variety of online IA training courses: http://iase.disa.mil/eta/online-catalog.html

- **Enterprise Mission Assurance Support Service (eMASS)** – Provides information about the DoD's recommended tool for automating the C&A process: http://www.disa.mil/Services/Information-Assurance/EMASS

- **Federal Information Security Management Act of 2002 (FISMA)** – A federal law requiring federal agencies to develop and implement information security programs for information systems that support the agency: http://csrc.nist.gov/drivers/documents/FISMA-final.pdf