Department of the Navy

DITSCAP to DIACAP

Transition Guide

9 June, 2008

Version 1.1

DOCUMENT CONFIGURATION CONTROL

Version	Release Date	Summary of Changes
1.0	15 May 2008	Original
1.1	9 June 2008	Minor change to 9 and 10 in the list in section 4.2

TABLE OF CONTENTS

LIST OF APPENDICES

LIST OF TABLES

1.0 EXECUTIVE SUMMARY

As of November 28, 2007, the Department of Defense (DoD) Information Assurance Certification and Accreditation Process (DIACAP) has replaced the DoD Information Technology System Certification and Accreditation Process (DITSCAP). All DoD Information Systems (IS) are required to transition to the DIACAP in accordance with instructions specified in Enclosure 5 of DoDI 8510.01.

The goal of the Department of the Navy (DON) Chief Information Office (CIO) is to ensure a smooth and successful migration of all DON ISs from DITSCAP to the DIACAP by the end of FY 2012. To initiate the implementation of DIACAP, all ISs are required to develop a strategy and plan for transition. This guide provides the necessary procedures for system and program owners to develop a transition plan to ensure adequate planning and coordination occurs for migration to DIACAP.

2.0 INTRODUCTION

The certification and accreditation (C&A) process is focused on the assessment and management of information security risk. The requirement to transition the DON from DITSCAP to DIACAP has afforded an opportunity to address several emerging community-wide challenges. The first is the increased criticality of ensuring all DON IS meet formal C&A requirements. The second is the requisite time, effort and documentation of the process virtually mandates that an automated solution be created to support C&A end-to-end. By providing automated support, early C&A stakeholder collaboration will ensure information security is addressed early in the development process.

To adequately plan for DIACAP transition and the requisite automation of the C&A process, DON established a DON DIACAP Working Group to develop a unified departmental transition plan to implement DIACAP. The approach undertaken includes:

- A formal DON DIACAP Transition Program to develop detailed guidance for implementing DIACAP within the DON
- Procurement and implementation of a DIACAP support system
- Guidance to assist all personnel involved in the security of IS in developing DITSCAP to DIACAP transition plans; i.e. the Program Managers (PM), Information Assurance Managers (IAM), and System Managers (SM)

2.1. PURPOSE

The purpose of this guide is to provide the DON with a department-wide transition strategy and detailed instructions on how to migrate systems and programs to the DIACAP in an orderly and efficient manner. It also provides the IS PM, SM, and IAM with the guidance, mandated by DoDI 8510.01, on how to plan for transition to DIACAP. It provides the processes and procedures for migrating unaccredited, new or DITSCAP-accredited systems to the DIACAP.

2.2. SCOPE

This guide applies to all ISs including IT systems, applications, networks, circuits, sites, infrastructure, enclaves, environments, and assets requiring security certification and accreditation within the DON, regardless of current accreditation status. For the purposes of this guide, the PM, SM, and IAM are the IA personnel responsible for the development and submission of the C&A package for an IS.

3.0 DON DIACAP TRANSITION STRATEGY

The DON CIO is responsible for the overall transition strategy, policies, and procedures. The actual execution of the strategy and procedures will be done by the individual services. Individual system/program/site transition planning is under the responsibility of the appropriate operational Designated Accrediting Authority (DAA). For the Navy, all operational systems are the responsibility of the Navy Operational DAA (ODAA) and for the Marine Corps, C4 Marine Corps Enterprise Network DAA (MCEN DAA).

3.1. DON DIACAP TRANSITION GOALS

The DON is committed to make the transition from DITSCAP to DIACAP as smooth as possible. Therefore, the transition will be implemented in phases so that C&A stakeholders are not unduly burdened throughout the process. Consistent with this approach, the following milestones are established:

- In the 3rd quarter of FY08:
  - DON CIO will release the DON DITSCAP to DIACAP Transition Guide.
  - DON CIO will release the DON DIACAP Handbook to provide a unified DON IA C&A process and to ensure continued Navy and Marine Corps alignment with respect to C&A activities.
  - DIACAP transition technical support will be established.
  - DIACAP Awareness Orientation will be initiated.
- Prior to full implementation of the new DON Certification and Accreditation Support Tool (CAST), DIACAP formatted C&A submissions will be processed using separate service specific submission systems and procedures. For the Navy, submissions will be processed using the current Information Assurance Tracking System (IATS) and the Marine Corps will use Xacta Information Assurance Manager.
- The DIACAP CAST implementation will begin in CY 2009.
- CAST training will begin after selection of the new tool and prior to the full DIACAP automation.
- All DON ISs will be fully transitioned to the DIACAP by FY2012.

3.2. DON DIACAP TRANSITION OVERVIEW

To fully migrate from DITSCAP to DIACAP five key components must be successfully executed.

- DIACAP transition planning must be conducted to provide the requisite management level information to predict and track C&A process resource requirements into the future.

- DIACAP awareness orientation must be provided to C&A professionals throughout the community to ensure an understanding of requirements and processes.
- Transition technical support must be available to answer questions that arise as PMs, SMs, and IAMs convert to DIACAP.
- An automated tool to support the end-to-end C&A process (i.e., CAST) must be successfully procured and implemented.
- CAST training will be required to familiarize the C&A community in the tool's capability and use to facilitate executing the DIACAP efficiently and effectively.

Each of these five components is described in detail in the following sections.

3.2.1. DIACAP TRANSITION PLANNING

Each system/site must develop a DIACAP transition plan detailing how it will obtain accreditation under DIACAP. Transition planning will accomplish several objectives:

- The individual (PM, SM, or IAM) responsible for the system/site will plan appropriate resources and schedules for transitioning.
- Allow C&A authorities (Certification Authority (CA); ODAA) to work with customers to determine the adequacy, realism, and fidelity of the approach to executing DIACAP requirements.
- Provide the necessary information for C&A authorities to plan for C&A package review resources.
- Provide metrics related information for training requirements development, CAST capability augmentation, and the identification of specific regional or environmental concerns.

All transition planning efforts will be coordinated by the respective service DAA upon the release of this DON DITSCAP to DIACAP Transition Guide. This coordination will independently evaluate requirements necessary to have systems/sites transition to DIACAP smoothly and efficiently, and will provide feedback to ISs on the planned transition timeline.

Specific guidance for DIACAP transition planning is found in section 4.0 below.

3.2.2. DIACAP AWARENESS ORIENTATION

The purpose of DIACAP Awareness Orientation is to introduce the strategy and methods to be used to train the personnel performing actions in the three main tiers of the C&A process – package creation, package review, and package approval.

A DIACAP awareness orientation briefing will be delivered to provide an introduction on how C&A will be conducted under DIACAP and steps needed to transition systems. Beginning 3rd Quarter FY08 high-level training will be provided to give an overview of DIACAP, the importance of accrediting all systems/sites and the importance of executing and maintaining C&A correctly. It will also provide the expected timeline for

transitioning a system or site to DIACAP based upon current accreditation status of the system or site.

When possible, this awareness orientation will be conducted in conjunction with IA conferences or symposiums where IA personnel are already gathered. In instances where this is not possible, stand-alone briefings will be conducted. Where capable, Video Teleconference (VTC) connections to remote locations will also be conducted.

3.2.3. TRANSITION TECHNICAL SUPPORT

DIACAP subject matter experts (SME) will be available to support PMs, SMs, and IAMs in planning each system's transition to DIACAP, including assistance in developing their respective transition plans and answering any related questions. SMEs will be available by email beginning 15 May 2008. Exact transition technical support contact information is provided in paragraph 5.0. Additional details on technical support will be provided via separate correspondence.

3.2.4. CERTIFICATION AND ACCREDITATION SUPPORT TOOL (CAST)

CAST will facilitate the transition to DIACAP in an effective and robust manner, automating the end-to-end C&A process. The tool will standardize end-to-end C&A processes for the DON enterprise and ensure a net-centric approach to risk evaluation with Information Assurance Control (IAC) inheritance. Specific goals include:

- Automate the implementation of the DIACAP process and procedures.
- Provide enterprise-wide visibility into security posture and risk acceptance.
- Provide robust metrics for continuous process improvement.

By automating the end-to-end C&A process, major requirements of the DIACAP will be accommodated. This includes:

- Ensuring IA is built in from the concept stage through the lifecycle.
- Inheritance of IACs.
- Enforcing annual reviews of all systems and sites.

By facilitating standardization and quality improvement of C&A packages from the initiation of the process, significant reductions in review times, rework, and learning curves will be realized. In addition, early collaboration by stakeholders will ensure adequate identification and resolution of issues early in the process and not during the formal C&A reviews.

Once the CAST procurement award is made, the automation will be initially implemented during a pilot phase with the objective of testing process, procedures, templates, etc. The pilot will build the necessary data bases, verify process steps, templates, and proper tool configuration, conduct test and evaluation, and process selected DIACAP C&A packages to verify tool effectiveness in a controlled environment. At the same time, training will be provided to the C&A community on the tool as well as the detailed DON processes and policies. It is expected that this training will be an on-going requirement throughout the life of CAST. Depending upon the tool selected, a

phased roll-out of service nodes may be needed in order to accommodate the planned deployment of the tool. Details will be provided following tool acquisition.

Because systems will begin transitioning to DIACAP prior to full implementation of the CAST, all submissions of C&A packages will continue using existing C&A package systems in the near term. For the Navy that is IATS and for the Marine Corps that is Xacta Information Assurance Manager. DIACAP templates can be found at https://www.fleetforces.navy.mil/netwarcom/navycanda/default.aspx

Once CAST is on-line for enterprise use, all accreditations (new, reaccreditations, and updates) must be processed through the CAST, which may require the transfer of data from legacy tools to the new tool by the system/site owners/managers or IAMS. Supplemental guidance for Service unique implementations may be provided, as required.

The current program schedule provides for fully automating DIACAP in 2009. DON CIO will issue a message announcing detailed milestones by the end of 2008.

3.2.5. DIACAP TRAINING

Once CAST is implemented, DIACAP training will target personnel performing activities in the three main tiers of the C&A process – package creation, package review, and package approval. The training will focus on the specific required tasks and how to perform these using the tool. Each tier will contain an overview of the DON process flow and build upon the activities accomplished by all members of the C&A team. Services retain the prerogative to tailor the training for their unique needs.

3.2.5.1 PM/IAM/SM

This level of training includes personnel performing initial and ongoing activities to implement the IACs, develop the certification package, including all artifacts, and maintain an accreditation. Roles at this level include a system PM, the system or local site IAM, the SM, and other supporting personnel including Information Assurance Officers (IAO), contractors and system administrators. These individuals prepare the package for submission, implement the IACs, and maintain IA situational awareness of the system throughout its life cycle and eventually conduct decommissioning activities.

3.2.5.2 Certifier/Validator/Echelon II/Major Subordinate Command (MSC)

This level of training involves the review of the package and the independent verification and validation of the proper implementation of IACs, culminating with an assessment of compliance with all security requirements, a risk level determination, and an accreditation recommendation. The Navy uses a centralized certifier or CA, while the Marine Corps uses local IA authorities (formerly identified as local DAAs) as Certifying Authority representatives (CARS).

3.2.5.3 DAA

This level of training comprises the DAA, including Operational DAA (ODAA), Developmental DAA (DDAA), Research and Development DAA (RDAA) and Local Site IA authorities such as Commanding Officers. This level conducts the final evaluation of

residual risk balanced with the operational need for the system and must determine if an authorization to operate, interim authorization to operate, or denial to operate is warranted.

4.0 DIACAP TRANSITION PLANNING

All DoD ISs are required to transition to the DIACAP in accordance with the timeline and instructions specified in Enclosure 5 of DoDI 8510.01 and as amplified in Table 1 below. The PM, SM or IAM for an IS is required to develop a plan for DON DIACAP transition, indicating when systems and sites will transition to DIACAP. C&A authorities will organize the department-wide transition, provide assistance to SMs/PMs/IAMs in transition planning, and prepare for DIACAP accreditation activities.

For planning purposes, major sites, bases, enclaves, circuits and computing facilities will need to be evaluated for IAC compliance in order to provide details for basic inheritance. These will be identified by the service operational DAAs (MCEN DAA and ODAA). This is necessary to provide the status of the technical and non-technical IAC compliance/non-compliance to support all systems, enclaves or programs of records installed. Additional guidance will be provided separately.

Systems without current accreditations should begin DIACAP immediately, following the guidelines contained in Table 1 below.

4.1. TRANSITION TIMELINE AND INSTRUCTIONS

Transition of DON IS assets from DITSCAP to DIACAP will take time and the DoDI 8510.01 allows DON C&A stakeholders the time necessary to determine an appropriate transition plan for the migration of each system.

The first step in building a transition plan is the identification of the C&A status of systems, programs, or sites. Definitively identifying this status, provides the PM, SM, or IAM with sufficient insight to build a plan for transition to DIACAP.

DON CIO has identified six C&A statuses and appropriate actions and timelines for a system, program or site to transition to DIACAP. The table below provides each C&A status with a general transition timeline and instructions. The PM, SM or IAM should select the condition that best identifies their current C&A status and pursue the general actions to be completed based on the status. If the PM, SM or IAM does not find a status that properly fits their system/program, the transition plan developer should contact the DIACAP Transition Technical Support discussed in paragraph 5.0 for further guidance.

Major sites, bases, enclaves, circuits and computing facilities may migrate as part of the initial CAST implementation beginning in 2nd quarter FY2009. While this happens, their current C&A status will remain valid. These ISs will be identified by the service operational DAAs (MCEN DAA and ODAA) to transition to DIACAP with the exact migration time determined through collaboration with the DAAs and IS owners as the program is implemented.

DON DIACAP implementation will continue with the release of the DON DIACAP Handbook. The handbook will contain the details that need to be followed to fully implement DIACAP for all ISs.

Table 1. DON DIACAP Transition Timeline and Instructions

DON IS C&A Status	Transition Timeline and Instructions
1. New start or unaccredited operational DON IS (No DITSCAP activity).	Initiate DIACAP. *Note 1: Operational systems without accreditation are subject to disconnection and/or decommissioning by DON CIO or the DAA.* *Note 2: Develop C&A documentation following DIACAP requirements and submit using Service specific process until CAST is available*
2. DON IS which has initiated DITSCAP, but does not yet have a signed Phase One System Security Authorization Agreement (SSAA).	Transition to DIACAP immediately. *Note 3: Services retain the prerogative to determine the course of action for each IS in this status.* *Note 4: Many of the documents and artifacts generated under DITSCAP will apply to DIACAP*
3. IS has a DITSCAP Phase One signed SSAA and is in Phase Two or Phase Three (does not yet have an accreditation decision). The Phase One SSAA Requirements Traceability Matrix (RTM) incorporates all DoD baseline IACs as specified in DoD Instruction 8500.2.	Continue under DITSCAP. The DITSCAP SSAA section addressing re-accreditation requirements shall be modified to identify and describe the system's strategy and schedule for transitioning to DIACAP, satisfying the DIACAP Annual Review and meeting the reporting requirements of the Federal Information Security Management Act (FISMA). The schedule for transitioning from DITSCAP to DIACAP shall not exceed the system re-accreditation timeline. *Note 5: The PM/SM/IAM shall perform the re-accreditation C&A steps under DIACAP.* *Note 6: If CAST is available and information from the current Service specific C&A system is needed for reaccreditation, that information must be converted and submitted to CAST by the*

DON IS C&A Status	Transition Timeline and Instructions
	PM/SM/IAM
4. IS has a DITSCAP Phase One signed SSAA and is in Phase Two or Phase Three (does not yet have an accreditation decision). The Phase One SSAA RTM does not incorporate all DoD baseline IACs as specified in DoD Instruction 8500.2.	Comply with guidance at #3 above and continue under DITSCAP. The DITSCAP RTM shall incorporate all DoD baseline IACs as specified in DoDI 8500.2 and a plan for implementing them shall be generated or modified. IAC implementation timelines may extend beyond the DITSCAP accreditation decision, that is, the DITSCAP accreditation decision is not contingent upon full compliance with the baseline IACs, but the system must provide information/visibility of compliance status and have a viable plan for achieving compliance in order to be granted an accreditation decision under DITSCAP. *Notes 5 & 6 apply*
5. IS has a DITSCAP accreditation decision that is current within 3 years.	Develop strategy and schedule for transitioning to DIACAP, achieving compliance with DoD Instruction 8500.2 baseline IACs, satisfying the DIACAP Annual Review, and meeting the reporting requirements of FISMA. If the DITSCAP RTM does not incorporate the baseline DoD IACs as specified in DoDI 8500.2, the DON IS shall provide the appropriate operational DAA with an assessment of compliance. If the accreditation decision is Interim Authority to Operate (IATO) and the system is on a path toward full authorization, continue under DITSCAP as modified by the guidelines of this table to achieve authorization. *Note 7: Once CAST is available, all C&A information will be submitted consistent with DIACAP requirements, including Annual Reviews, re-accreditation submissions, etc. Note 6 above applies*
6. IS has a DITSCAP Authority To Operate (ATO) that is more than 3 years old.	Initiate DIACAP. *Note 8: Operational systems without accreditation are subject to disconnection*

DON IS C&A Status	Transition Timeline and Instructions
	and/or decommissioning by the DAA. Notes 1 through 7 apply.

4.2. TRANSITION PLAN DEVELOPMENT

The transition plan is used to capture the basic information on the IS to allow identification and tracking throughout the transition period. At a minimum, transition planning will consider the system/program/site details and transition schedule.

Specific details for transition planning and plan development will be coordinated by the appropriate service operational DAA via separate correspondence.

The entire DIACAP process including documents and templates are contained in the DON DIACAP Handbook which will be released separately in June 2008.

An example of the type of information needed for transition planning is provided below. The actual format and details will be provided by the appropriate service operational DAA.

Examples of transition planning information:

1. System/Site Name – official name of system or site being accredited
   Version – version or release identification
   Acronym – the acronym for system or site being accredited
2. System/Site Description – a brief narrative description of the system/site, its function, and uses.
3. DITPR-DON ID Number – provide the number if applicable. If not applicable, mark N/A.
4. FAM Status – status of the Functional Area Manager (FAM) approval of system to operate in DON. Statuses include: Approved, Disapproved, Allowed with Restrictions, etc.
5. DADMS ID Number – the ID number for the system in DADMS
6. System Life Cycle or Acquisition Phase - What part of the life cycle or what acquisition phase is the system or program in: Concept, Milestone A, B, C, Production & Development, Operations & Support, or other?
7. Information System Type – is the IS a site, system, application, circuit, PIT interconnection, network, or enclave)? Is the IS operational, developmental, research, demonstrative, etc.?
8. Enclave the System/Site in part of – what enclave, MAN, BAN or Site LAN is the system part of (NIPRNet, SIPRNet, NMCI, ONENet, ISNS, MCEN, MCTN, legacy, etc)?
9. List of sites where system is installed – this is for systems, applications, networks, circuits, infrastructures, enclaves, or environments only - list all sites (i.e. buildings, campuses, facilities, bases, locations, etc.) where the system is installed. If this plan is for a site, mark this as N/A.
10. List of systems installed at the site – this is for sites only – list all systems, applications, networks, circuits, infrastructures, enclaves, or environments installed at the site. If this plan is for a system, mark this as N/A.

11. Accreditation Status – is the accreditation of the system/site current, expired, presently unaccredited, or never accredited?
12. Type of Accreditation Issued – what accreditation was issued to the system: IATO, IATT, ATO, other?
13. Accreditation Termination Date – expiration date of the current accreditation (IATO, IATT, ATO, etc.) expires. (DD-MMM-YYYY).
14. Governing DON Service IA Program – Which DON service (Navy or Marine Corps) has accreditation responsibility for the system or site?
15. Responsible Service DAA – which DAA has cognizance over this system or site (Navy ODAA, MCEN DAA, DDAA, RDAA, other)?
16. Echelon II/MSC Name – the command/unit/organization name of the echelon II or Major Subordinate Command (MSC) responsible for the system or site.
17. Echelon II/MSC POC Name – the point of contact in the echelon II/MSC responsible for system or site.
18. Echelon II/MSC POC Email - the email address for the echelon II/MSC point of contact responsible for system or site.
19. Echelon II/MSC POC Phone - the phone number for the echelon II/MSC point of contact responsible for system or site.
20. System/Site Command Name – the command/unit/organization name of the owners/managers of the system or site being covered in this plan.
21. UIC – the Unit Identification Code (UIC) of command/unit/organization which owns and manages the system/site in this plan.
22. PM/SM/IAM Name – the full name of the PM//SM/IAM of system/site.
23. PM/SM/IAM Email – the email address of the PM/SM/IAM of system/site.
24. PM//SM/IAM Phone – the phone number of the PM/SM/IAM of system/site.
25. System/Site Transition Plan/Schedule - provide a written description of the plan and schedule for transition of the system and program by describing:
    - Date current accreditation was issued.
    - Date of Submission of the DIACAP Transition Plan.
    - The current IS status (found in Table 1)
    - Planned date for start of transition (i.e. based on the system C&A status in Table 1)
    - Expected date for submission of DIACAP compliant accreditation package.
    - Planned accreditation date under DIACAP (i.e. when the system/program will need to be accredited?)
    - The high-level steps required to get the system accredited under DIACAP, including those significant events that will impact the plan and should be highlighted for C&A stakeholders

4.3. REVIEW OF TRANSITION PLANNING

Once the transition planning is complete, the appropriate service operational DAA will coordinate review of the transition planning. Some of the goals of transition planning review are:

- Ensure the system or program can transition to DIACAP smoothly and efficiently

- Allow DAAs to provide feedback to PMs, SMs, and IAMs on their planned transition timeline
- Capture information for enterprise planning purposes
- Resolve transition issues through stakeholder collaboration

Submission and review of transition plans will be coordinated by the appropriate service operational DAA

5.0 Transition Technical Support

DIACAP SMEs will be available to support PMs, SMs, and IAMs in the planning of systems transition to DIACAP, including assistance in developing the transition plans and answering any questions regarding the transition. Primary contact for DITSCAP to DIACAP transition technical support is at:

- SPSC-DON-DIACAP@navy.mil

All efforts should be made to contact the primary technical support contact first.

Secondary contacts for transition technical support are:

- Navy
  - Operational DAA (ODAA)
  - Email: Navy_ODAA@navy.mil
  - Phone: (757) 417-6719 x0
- Marine Corps
  - Programs of Record (not yet fielded), contact the MCSC C4 II
  - All other systems (including fielded PORs), contact the MCEN DAA
    - Email: M_MCEN_DAA@usmc.mil
    - Phone: (703) 693-3490

APPENDIX A: REFERENCES

DoDI 8510.01, DoD Information Assurance Certification and Accreditation Process (DIACAP), 28 November 2007.

SECNAV M-5239.1. “Information Assurance Manual,” November 2005. (Copies of this document are available online at http://doni.daps.dla.mil/SECNAV%20Manuals1/5239.1.pdf

DoD Directive 8500.1E, “Information Assurance (IA),” 24 Oct 2002. (Copies of this document are available online at http://www.dtic.mil/whs/directives/or ASDNII.pubs@osd.mil.)

DoD Instruction 8500.2, “Information Assurance (IA) Implementation,” 6 February 2003. (Copies of this document are available online at http://www.dtic.mil/whs/directives/corres/ins1.html or ASDNII.pubs@osd.mil.)

APPENDIX B: DEFINITIONS

Term	Definition
Accreditation	Formal declaration by the DAA that an IS is approved to operate in an acceptable level of risk, based on the implementation of an approved set of technical, managerial and procedural safe-guards.
Accreditation Decision	A formal statement by a designated accrediting authority (DAA) regarding acceptance of the risk associated with operating a DoD information system (IS) and expressed as an authorization to operate (ATO), interim ATO (IATO), interim authorization to test (IATT), or denial of ATO (DATO). The accreditation decision may be issued in hard copy with a traditional signature or issued electronically signed with a DoD public key infrastructure (PKI)-certified digital signature.
Application	Software program that performs a specific function directly for a user and can be executed without access to system control, monitoring or administrative privileges. Examples include office automation, electronic mail, web services, and major functional or mission software programs.
Artifacts	System policies, documentation, plans, test results and the like that express or enforce the IA posture of the DoD information system, make up the C&A information, and provide evidence of compliance with the assigned IA Controls
Assigned IA Controls	A list of IA Controls that a DoD information system must address to achieve an adequate IA posture. Assigned IA Controls include baseline DoD IA Controls, optional DoD IA Controls for special conditions or technologies, e.g., health information portability and privacy or cross security domain solutions, and DoD, Mission Area, Component and DoD information system supplements, if any.
Authorization to Operate (ATO)	The authorization granted by a DAA, for a DoD IS to process, store, or transmit information. An ATO indicates a DoD IS has adequately implemented all assigned IACs to the point where residual risk is acceptable to the DAA. Authorization is based on acceptability of the IA component, the system architecture, and implementation of assigned IA Controls.
Automated Information System (AIS)	Set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. Includes AIS applications, enclaves, outsourced IT-based processes, and platform IT interconnections.
Base Area Network (BAN)	A base-area network is a computer network covering a military geographic area, like a post, station, base, or group of buildings e.g. a facility or campus. The defining characteristics of BANs, in contrast to wide-area networks (WANs), include their smaller geographic range.
Certification	Comprehensive evaluation of the technical and non-technical security safeguards of an IS to support the accreditation process

Term	Definition
	that establishes the extent to which a particular design and implementation meets a set of specified security requirements.
Certification & Accreditation Support Tool (CAST)	The DON DIACAP C&A support system designed to automate the C&A process.
Certifying Authority (CA)	An official responsible for performing the comprehensive evaluation of the security features of an information system and determining the degree to which it meets its security requirements
Circuit	A conglomeration and interconnection of electronic components with a number of channels to provide a communication path or network for one-way or two-way communications. Usually a pair of channels providing bidirectional communication. More or less interchangeable with "network".
Designated Accrediting Authority (DAA)	Official with the authority to formally assume the responsibility for operating a system at an acceptable level of risk. This term is synonymous with authorizing official, designated approving authority and delegated accrediting authority.
Developmental Designated Accrediting Authority (DDAA)	The DDAA is the official responsible for ensuring completion of the DAA function of C&A for applications or systems during acquisition, development, Certification Test and Evaluation (CT&E) and risk mitigation prior to use or testing within the operational Naval enterprise.
DIACAP Package	The collection of documents or collection of data objects generated through DIACAP implementation for an information system. A DIACAP package is developed through DIACAP activity and maintained throughout a system's life cycle. Information from the package is made available as needed to support an accreditation or other decision such as a connection approval. The executive package for a DAA or CIO includes the System Information Profile (SIP), the DIACAP Scorecard, and the POA&M for an information system. The comprehensive package includes the SIP, the DIACAP Scorecard, and the POA&M, as well as the following for each assigned IA Control: the assigned IA Controls; implementation material from the DIACAP Knowledge Service including implementation guidance; validation procedures and expected results for the assigned IA Controls; whether the IA Control is inherited or its implementation status; actual validation results; applicable associated documentation/artifacts; the responsible entities, resources, and estimated completion dates, as applicable.
DIACAP Scorecard	A summary report that shows the certified or accredited implementation status of a DoD information system's assigned IA Controls and supports or conveys a certification determination and/or accreditation decision.
DoD Information Assurance Certification and	A life cycle process for identifying, implementing, validating, certifying, and managing IA capabilities and services, expressed as IA Controls, and authorizing the operation of DoD information

Term	Definition
Accreditation Process (DIACAP)	systems in accordance with statutory, Federal and DoD requirements.
DoD Information System	Set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. Includes AIS applications, enclaves, outsourced IT-based processes, and platform IT interconnections.
DoD Information Technology Portfolio Repository – Department of the Navy	DITPR-DON is the DON variant of DoD IT Portfolio Registry (DITPR) that is used to record investment review and certification submission information, FISMA assessments, E-Authentication status, and Privacy Impact Assessment status.
DON Application and Database Management System (DADMS)	The database managed by the DON and the Functional Area Managers (FAM) designed as a repository to store, track and approve applications, databases, systems, and networks for operation with in the DON.
DoD Information System	DoD set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information.
DoD Information Technology Security Certification and Accreditation Process (DITSCAP)	The standard DoD process for identifying information security requirements, providing security solutions, and managing IS security activities.
Enclave	Collection of computing environments connected by one or more internal networks under the control of a single approval authority and security policy, including personnel and physical security.
Federal Information Security Management Act (FISMA)	The FISMA requires Federal departments and agencies develop and implement an organization-wide information security program designed to safeguard IT assets and data. It lays out the Federal framework for annual IT security reviews, reporting, and remediation planning; and it requires that Federal departments and agencies evaluate their information system security programs and report the results on an annual basis. Under FISMA, the term 'information security' means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, which means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity; confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and availability, which means ensuring timely and reliable access to and use of information.
Information Assurance (IA)	Measures that protect and defend information and ISs by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection,

Term	Definition
	detection and reaction capabilities.
Information Assurance Control (IAC)	An objective IA condition of integrity, availability, or confidentiality achieved through the application of specific safeguards or through the regulation of specific activities that is expressed in a specified format (i.e., a control number, a control name, control text, and a control class). Specific management, personnel, operational, and technical controls are applied to each DoD information system to achieve an appropriate level of integrity, availability, and confidentiality in accordance with DoDI 8500.2
Information Assurance Manager (IAM)	Individual responsible for a program, organization, system, or enclave's information assurance program.
Information System (IS)	Set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display or transmission of information. Any telecommunication or computer-related equipment or interconnected system or subsystems of equipment that is used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of voice and/or data, and includes software, firmware, and hardware.
Information Assurance Tracking System (IATS)	The Navy C&A repository, process and tracking tool.
Inheritance	Inheritance in the context of DIACAP refers to the state in which an IA Control along with the control validation results and compliance status is shared across two or more systems for the purposes of C&A. Through inheritance, an existing IA Control and its C&A status, would extend from an "originating" system to another "receiving" system in order to model a real-word scenario of shared security infrastructure or capability. Inheritance is intended to reduce the complexity of testing by allowing the unilateral application of validation test results to all systems sharing the security capability. The DIACAP Implementation Plan specifically identifies IA Controls inherited between systems.
Interim Approval to Operate (IATO)	Temporary authorization to operate a DoD IS under the conditions or constraints enumerated in the accreditation decision.
Interim Approval to Test (IATT)	Temporary approval to test a DoD information system in a specified operational information environment within the timeframe and under the conditions or constraints enumerated in the accreditation decision.
Metropolitan Area Network (MAN)	A MAN is a computer network covering a large military geographic area, like a grouping of posts, stations, or bases. A network that uses routers and public communications links for a specific metropolitan area (e.g., a city) respectively. The defining characteristics of MANs, in contrast to wide-area networks (WANs), include their smaller geographic range. .
Plan of Action and	A plan of action and milestones required for any accreditation

Term	Definition
Milestones (POA&M)	decision that requires corrective actions. The POA&M addresses: (1) why the system needs to operate; (2) any operational restrictions imposed to lessen the risk during the interim authorization; (3) specific corrective actions necessary to demonstrate that assigned IA Controls have been implemented correctly and are effective; (4) the agreed upon timeline for completing and validating corrective actions; and (5) the resources necessary and available to properly complete the corrective actions.
Platform IT Interconnection	For DoD information assurance purposes, platform IT interconnection refers to network access to platform IT. Platform IT interconnection has readily identifiable security considerations and needs that must be addressed in both acquisition, and operations. Examples of platform IT interconnections that impose security considerations include remote administration and remote upgrade or reconfiguration.
Program or System Manager (PM or SM)	Official responsible for the overall procurement, development, early and seamless integration of IA, modification, operation and maintenance of an assigned DON IS throughout the system life cycle.
Risk Management	Process concerned with the identification, measurement, control, and minimization of security risks in IT systems to a level commensurate with the value of the assets protected. Achieving and maintaining an acceptable IA posture (i.e., adequate security, interoperability, and visibility within IA situational awareness or command and control systems) through the implementation of assigned IACs. IACs are assigned based on the value of the information being processed and the extent of information environment being shared.
Site	One or more information systems under the control of a single IAM is termed a site. A site may include more than one facility or location (e.g., building, campus or base) provided those locations under the purview of the IAM. A site consists of one or more security domains. Sites may have additional security domains containing other classifications, coalition partner information. Each security domains contains one or more enclaves. An enclave is a collection of computing environments connected by one or more internal networks. Security domains are a logical grouping of systems based on security policy. Enclaves are a grouping of systems based on a physical characteristic such as location or connectivity. Enclaves are characterized by their membership in a security domain. This membership may be temporal in the case of periods processing.
Site Accreditation	The accreditation of one or more information systems under the control of an IAM and operational DAA as a single accreditation is termed site accreditation. Site accreditation combines the system specific information from C&A packages developed under DoD IA C&A policies into an integrated IA document describing that site

Term	Definition
	and the security controls common to the domains at that site.
System	A set of interrelated components consisting of mission, environment, and architecture as a whole. See also Automated Information System (AIS) , DoD Information System, and Information System (IS)
System Identification Profile (SIP)	An information base, i.e., a document, collection of documents, or collection of data objects within an automated IS, that uniquely identifies an information system within the DIACAP and contains established management indicators, e.g., DIACAP status.
System Owner (SO)	A System Owner (SO) is any entity who has the responsibility to develop and field a IS within the DON. In IA the SO has the same role, responsibilities and requirements as a PM.
User Representative (UR)	Individual or organization that represents the user community in the DIACAP.
Validator	Entity responsible for conducting a validation procedure.
Wide Area Network (WAN)	A computer network that covers a broad area (i.e., any network whose communications links cross metropolitan, regional, or national boundaries. The largest and most well-known DoD example of a WAN is the NIPRNet.

APPENDIX C: ACRONYMS

ACRONYM	DEFINITION
AIS	Automated Information System
ATO	Approval to Operate
BAN	Base Area Network
C&A	Certification & Accreditation
C4	Command, Control, Communications, and Computers
CA	Certifying Authority
CAST	Certification And Accreditation Support Tool
CIO	Chief Information Officer
DAA	Designated Accrediting Authority
DADMS	DON Application and Database Management System
DDAA	Developmental Designated Accrediting Authority
DIACAP	DoD Information Assurance Certification and Accreditation Process
DISN	Defense Information Systems Network
DITPR-DON	DoD Information Technology Portfolio Repository – Department of the Navy
DITSCAP	DoD Information Technology Security Certification and Accreditation Process
DoD	Department of Defense
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
DON	Department of the Navy
FAM	Functional Area Manager
FISMA	Federal Information Security Management Act
FY	Fiscal Year
IA	Information Assurance
IAC	Information Assurance Control
IAM	Information Assurance Manager
IAO	Information Assurance Officers
IATO	Interim Approval to Operate
IATS	Information Assurance Tracking System
IATT	Interim Approval to Test
IS	Information System
ISNS	Integrated Shipboard Network System
ISSE	Information Systems Security Engineering
IT	Information Technology
LAN	Local Area Network
LSS	Lean-Six-Sigma
MAN	Metropolitan Area Network
MCEN	Marine Corps Enterprise Network
MSC	Major Subordinate Command
MCTN	Marine Corps Tactical Network
NIPRNET	Non-Classified Internet Protocol Router Network
NMCI	Navy Marine Corps Intranet
ODAA	Operational Designated Accrediting Authority
ONENet	OCONUS Naval Enterprise Network
PM	Program Manager
POA&M	Plan of Action and Milestones
POC	Point of Contact
RDAA	Research and Development Designated Accrediting Authority
RTM	Requirements Traceability Matrix
SECNAV	Secretary of the Navy
SIP	System Identification Profile
SIPRNET	Secret Internet Protocol Router Network
SM	System Manager
SME	Subject Matter Expert

ACRONYM	DEFINITION
SO	System Owner
SSAA	System Security Authorization Agreement
ST&E	Security Test & Evaluation
UIC	Unit Identification Code
VTC	Video Teleconference