Headquarters Marine Corps
Command, Control,
Communications, and Computers (C4)
Information Assurance Division

Marine Corps Enterprise Information Assurance Directive

018 Marine Corps Certification and Accreditation Process

V 2.0

2 September 2008

FOR OFFICIAL USE ONLY

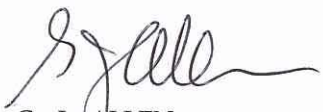
This page intentionally left blank

FOREWARD

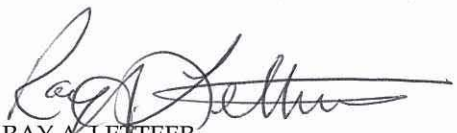
The Marine Corps Enterprise Network (MCEN) Designated Accrediting Authority (DAA) issues Marine Corps Enterprise Information Assurance Directives (EIAD). The EIAD series provides modules that guide the implementation of policy direction established in Marine Corps Order (MCO) 5239.2. The modules provide procedural, technical, administrative, and supplemental guidance for all information systems, used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or receipt of data within the MCEN as well as other Marine Corps information systems. Each module focuses on a distinct subject and describes a standard methodology for planning, implementing and executing an element of the Marine Corps Information Assurance Program (MCIAP). The Marine Corps EIAD series will be the authoritative source for implementation of IA policy direction.

This module, *"Marine Corps Certification and Accreditation Process,"* addresses certification and accreditation requirements and standards and serves as direction for users of Marine Corps Information Systems and Information Technology Resources.

Reviewed and Approved by:



G. J. ALLEN
BRIGADIER GENERAL, U.S. MARINE CORPS
DIRECTOR, COMMAND, CONTROL, COMMUNICATIONS, AND COMPUTERS



RAY A. LETTEER
MARINE CORPS ENTERPRISE NETWORK DAA
DIRECTOR, COMMAND, CONTROL, COMMUNICATIONS, AND COMPUTERS
INFORMATION ASSURANCE DIVISION

Document Configuration Control

Version	Release Date	Summary of Changes
Versions 0.1 – 0.92	August 3, 2007	Developmental Draft Versions
Version 0.93	September 4, 2007	Updated with comments from MCSC and MCNOSC
Version 0.94	October 30, 2007	Updated graphics, corrected grammar
Version 0.95	November 8, 2007	Updated with comments from Operating Forces
Version 1.0	November 13, 2007	Finalized for approval
Version 2.0	September 2, 2008	Modified to reflect the implementation of DIACAP by the Marine Corps

TABLE OF CONTENTS

EXECUTIVE SUMMARY VIII

1.0 INTRODUCTION 1

1.1 BACKGROUND 1
1.2 PURPOSE 1
1.3 APPLICABILITY AND SCOPE 2
1.4 CANCELLATION 3
1.5 DISTRIBUTION 3
1.6 STRUCTURE 4
1.7 RECOMMENDATIONS 4
1.8 EFFECTIVE DATE 4

2.0 POLICY 5

MARINE CORPS POLICY ON C&A 5
2.1 INFORMATION TECHNOLOGY (IT) PROCUREMENT AND C&A 6

3.0 CERTIFICATION & ACCREDITATION OVERVIEW 7

3.1 WHAT IS CERTIFICATION &ACCREDITATION? 7
3.2 UNIQUE ACCREDITATIONS 10
3.3 WHY IS C&A IMPORTANT? 12
3.4 C&A LIFE CYCLE 12
3.5 C&A MAINTENANCE 13
3.6 C&A DOCUMENTATION 13

4.0 ROLES AND RESPONSIBILITIES 14

4.1 HEADQUARTERS MARINE CORPS C4 CIO 15
4.2 SENIOR IA OFFICIAL (SIAO) 15
4.3 DESIGNATED ACCREDITING AUTHORITY (DAA) 16
4.4 CERTIFYING AUTHORITY 21
4.5 PROGRAM MANAGER 25
4.6 IA MANAGERS/OFFICERS (IAM/IAO) AND INFORMATION SYSTEM SECURITY ENGINEER (ISSE),26
4.7 COMMANDERS 30
4.8 USER REPRESENTATIVES (UR) 31

5.0 MARINE CORPS C&A PROCESS (MCCAP) 32

5.1 INITIATE AND PLAN IA C&A 36
5.2 IMPLEMENT AND VALIDATE ASSIGNED IA CONTROLS 43
5.3 MAKE CERTIFICATION DETERMINATION AND ACCREDITATION DECISION 51
5.4 MAINTAIN AUTHORITY TO OPERATE AND CONDUCT REVIEW 58
5.5 DECOMMISSION 61

6.0 CIRCUIT CONNECTION APPROVAL DOCUMENTATION 62

6.1 IAM/IAO: 62

6.2 COMMAND G-6 (CA REPRESENTATIVE): 62
6.3 MCEN DAA AND SUPPORT STAFF: 63
7.0 REFERENCES 64
ENCLOSURE A – ACRONYMS 67
ENCLOSURE B - SAMPLE CAR ASSIGNMENT LETTER 70
ENCLOSURE C - SAMPLE IAM/IAO ASSIGNMENT LETTER 70
ENCLOSURE D - NIPRNET CIRCUIT QUESTIONNAIRE (NCQ) 76
ENCLOSURE E - SIPRNET CIRCUIT QUESTIONNAIRE (SCQ) 79

TABLE OF FIGURES

Figure 1 - System Accreditation Model 7
Figure 2 - Type Accreditation Model 8
Figure 3 - Site Accreditation Model 10
Figure 4 - DIACAP Activities Mapped to Acquisition Cycle 19
Figure 5 - DoD C&A Process Cycle 32
Figure 6 - Marine Corps C&A Process Diagram 34
Figure 7 - Initiate DIACAP Package Workflow 36
Figure 8 - Implement and Validate IA Controls 43
Figure 9 - Make Certification and Accreditation Decision 51
Figure 10 - Maintain Authority to Operate and Conduct Review 58
Figure 11 - Decommission Information System 61

EXECUTIVE SUMMARY

Under current Federal Certification and Accreditation (C&A) requirements, an information system (IS) is required to undergo a formal accreditation process at least once every three years or when major modifications occur that affect the systems security posture. This Directive provides a standardized approach to obtaining an accreditation decision for United States Marine Corps IS as required under federal law, Department of Defense, and the Department of the Navy regulations and directives.

The formal C&A process, with associated documentation, provides evidence of a risk mitigation methodology that complies with Marine Corps, Department of the Navy, Department of Defense, National Institute of Standards and Technology (NIST), and Federal standards, laws, and regulations. This program will help define measures of performance used to assure that IS implement and test adequate Information Assurance Controls (IAC), that risks are assessed, and that DIACAP Packages are maintained.

This Directive maps out the tasks and subtasks to be completed to allow for an accreditation decision to be made by the appropriate authority. This is known as the C&A process.

This page intentionally left blank

1.0 INTRODUCTION

1.1 BACKGROUND

This Marine Corps Enterprise IA Directive, *Marine Corps Certification and Accreditation* is intended to provide a comprehensive and uniform approach to the certification and accreditation (C&A) process for the United States Marine Corps, to include all subordinate commands, bases, and organizations. Individuals responsible for, or involved in the C&A process, will use this Directive as a resource to certify and accredit United States Marine Corps's (Marine Corps) networks, networked systems, network components, and individual systems, hereafter identified as information systems (IS).

This Directive denotes policy and establishes a standard process for all Marine Corps organizations and commands, and identifies a set of activities, general tasks, and management structure to certify and accredit systems that will maintain the information assurance (IA) and security posture of a system, network or site. Beyond defining a process, this Directive will also address several fundamental questions related to the C&A process.

The Federal Information Security Management Act of 2002 (FISMA)[1] consolidated many federal security policies and mandates into a single law and required an annual assessment to track compliance with those regulations. FISMA gives Congress permanent oversight of agency security matters and expands the information that agencies must submit to Congress, including plans for fixing security problems. FISMA requires agencies to follow security standards developed by the NIST. FISMA also requires agency chief information officers to perform self-assessments and inspectors general to perform independent assessments annually on the effectiveness of agencies' security programs, any deficiencies and the progress of any corrective actions.

DoDD 8500.1, *Information Assurance (IA)*, and DoDI 8500.2, *Information Assurance (IA) Implementation*, require certification and accreditation of most DoD ISs in accordance with DoDI 8510.01, *DoD Information Assurance Certification and Accreditation Process* (DIACAP), or DCI Directive 6/3, *Protecting Sensitive Compartmented Information within Information Systems*, as appropriate.

1.2 PURPOSE

Using the C&A methodology defined in this Directive will result in a standardized C&A program across Marine Corps. Proper use of the C&A methodology will assure Marine Corps leadership that the level of security implemented and controls in place adequately protects assets given an acceptable level of residual risk. Organizations and

---

[1] *P.L. 107-347*

commands within Marine Corps will benefit from the C&A activities performed on their systems in the following ways—

- Standard operating environment through utilization of baseline security requirements
- Clearly defined system boundaries
- Documented DIACAP Implementation Plans
- Defined contingency plans
- Established configuration management processes
- Heightened information security (INFOSEC) awareness
- Validated security controls
- Measured levels of risk based on identified threats and vulnerabilities
- Uniform system and network inventory (i.e., information sensitivity and mission criticality levels)
- Defined security roles and responsibilities
- Formal Authorization to Operate (ATO).

This Enterprise IA Directive establishes the Marine Corps Certification & Accreditation Process (MCCAP) for accrediting ISs for operation within Marine Corps environments and supports net-centricity through an effective and dynamic C&A Process. DoD policy requires that all DOD Information Technology (IT) systems maintain an appropriate level of confidentiality, integrity, authentication, non-repudiation, and availability. The MCCAP provides visibility and control of the implementation of IA capabilities and services, the certification & accreditation (C&A) process, and accreditation decisions authorizing the operation of ISs. This is accomplished through the implementation of the DIACAP process. The directive supports the foundation of the DIACAP process.

1.3 APPLICABILITY AND SCOPE

1.3.1 Applicability

This Directive applies to:

- All Marine Corps organizations including the operating forces and supporting establishment.

- All Marine Corps owned or controlled ISs that receive, process, store, display, or transmit USMC or USMC supporting information, throughout the entire system life cycle (SLC) regardless of classification or sensitivity.
- Marine Corps ISs that support special environments, e.g., Special Access Requirements (SARs), as supplemented by the special needs of the program.
- ISs under contract to the Marine Corps.
- ISs of Non-appropriated Fund Instrumentalities.
- Stand-alone ISs.
- Mobile computing devices such as laptops, handhelds, and personal digital assistants operating in wired or wireless mode, and other information technologies as may be developed.
- Marine Corps ISs that are prototypes or Advanced Concept Technology Demonstrations (ACTDs).

1.3.2 Scope

The scope of this Directive includes defining the MCCAP, describing why C&A is important, illustrating how C&A maps to the System Development Life Cycle (SDLC), identifying roles and responsibilities of key players, explaining types of C&A recommendations and decisions, and describing the five DIACAP activities that comprise the MCCAP.

Nothing in this Directive shall alter or supersede the existing authorities and policies of the Director of National Intelligence (DNI) regarding the protection of Sensitive Compartmented Information (SCI) and special access programs for intelligence as directed by Executive Order 12333 and other laws and regulations. The application of the provisions and procedures of this Instruction to SCI or other intelligence ISs is encouraged where they may complement or address areas not otherwise specifically addressed.

1.4 CANCELLATION

This document cancels the Marine Corps Enterprise Information Assurance Directive 018, *Marine Corps Certification and Accreditation Process*, version 1.

1.5 DISTRIBUTION

This document is approved for limited distribution. Department of Defense (DoD) components (including the combatant commands) and other federal agencies may obtain copies of this Directive through controlled Internet access only (limited to .mil and .gov users). Copies are available at: https://hqdod.hqmc.usmc.mil/c4/IA.asp.

1.6 STRUCTURE

This Directive is organized into six major sections. Section 1 provides an introduction to the Marine Corps Certification and Accreditation Process. Section 2 is the Marine Corp's policy regarding the requirement for certifying and accrediting ISs before being granted authority to operate. Section 3 provides an overview of the C&A process and how the Federal standards apply to specific classes of Marine Corps systems. Section 4 outlines the roles and responsibilities in the C&A process, with focus on unique Marine Corps positions. Section 5 translates the DIACAP process as it applies to the special business and mission cases within the Marine Corps. This section is of particular use for anyone in the Marine Corps desiring to begin the C&A effort immediately. Section 6 provides an overview on procedures for acquiring an approval to connect to the Global Information Grid (GIG) backbone.

1.7 RECOMMENDATIONS

Recommendations for change or amendment to this Directive may be submitted in writing through the HQMC C4 IA Division. Recommendations will be evaluated and coordinated with the appropriate Marine Corps organizations before the change or amendment is instituted by the HQMC C4 IA Division.

1.8 EFFECTIVE DATE

This Enterprise IA Directive is effective as of its signature date.

2.0 POLICY

MARINE CORPS POLICY ON C&A

Based on DoD policy, it is Marine Corps policy that the Marine Corps shall certify and accredit ISs through an enterprise process for identifying, implementing, and managing IA capabilities and services. The Marine Corps shall establish and use a service enterprise decision structure for the MCCAP as described herein.

The MCCAP shall support the transition of ISs to GIG standards and a net-centric environment while enabling assured information sharing by:

- Providing a standard C&A approach
- Managing and disseminating service enterprise standards and guidelines for IA design, implementation, configuration, validation, operational sustainment, and reporting. These standards and guidelines can be accessed at: https://hqdod.hqmc.usmc.mil/IA/Pages/Orders.asp
- Accommodating diverse ISs in a dynamic environment

All Marine Corps–owned, -controlled or –supporting ISs shall be under the governance of the Marine Corps IA Program (MCIAP) and fall under the Marine Corps Network Operations & Security Center (MCNOSC) Computer Network Defense (CND) service provider. This does not include systems processing special compartmented information. The MCIAP shall be the primary mechanism for ensuring enterprise visibility and synchronization of the MCCAP.

All Marine Corps IS programs shall create a DIACAP Package using the specified automated tool for the MCCAP. This enables Program Managers (PM), and Information Assurance Managers (IAM) within the Marine Corps to determine the scope and state of all IA activities within the MCEN in order to identify IA requirements, develop policy, manage and train personnel, and make decision concerning acquisition, IA resources and programming.

All Marine Corps ISs shall be implemented using the baseline DoD IA controls in accordance with DoDI 8500.2 for unclassified, sensitive, and collateral classified information. The baseline DoD IA controls may be augmented, but not reduced, if required to address localized threats or vulnerabilities. Systems processing SCI must follow appropriate Intelligence Community (IC) directives.

The C&A status of all Marine Corps ISs shall be made available to support MCEN Designated Accrediting Authority (DAA) accreditation decisions. By definition, the MCEN is defined as all Marine Corps voice and data networks and ISs including wired

or wireless, in garrison or deployed, that process, store, and/or transmit Marine Corps information.

All Marine Corps ISs with an Authorization to Operate (ATO) shall be reviewed at least annually to ensure that assigned IA controls remain valid and effective.

Resources for implementing the MCCAP shall be identified and allocated as part of the Defense Planning, Programming, Budgeting, and Execution (PPBE) process, and reported to HQMC C4 IA.

Provisions for implementing the MCCAP shall be written into contracts of applications, systems, services, and programs that are required to comply with the MCCAP. Failure to meet this requirement may be used as justification for MCCAP non-compliance.

2.1 INFORMATION TECHNOLOGY (IT) PROCUREMENT AND C&A

DoDI 8580.1, *Information Assurance in the Defense Acquisition System*, implements policy, assigns responsibilities, and prescribes procedures necessary to integrate IA into the Defense Acquisition System. The Instruction also describes required and recommended levels of IA activities relative to the acquisition of systems and services, and describes the essential elements of an Acquisition IA Strategy process. The required IA activities include C&A actions.

3.0 CERTIFICATION & ACCREDITATION OVERVIEW

3.1 WHAT IS CERTIFICATION &ACCREDITATION?

Certification is a comprehensive evaluation of the technical and non-technical security features and other safeguards of an IT system and establishes the extent to which a particular design and implementation meets documented security requirements.

Accreditation is the formal declaration by an approving authority that an IT system is compliant with established security requirements and is approved to operate using a prescribed set of safeguards. This decision is strongly based on the residual risks identified during certification.

There are different types of accreditation depending on what is being certified.

- A system accreditation evaluates a particular system, i.e., hardware, software, and firmware.
- A type accreditation evaluates systems or networks with identical environments that are distributed to a number of different locations.
- A site accreditation evaluates the applications and systems at a specific, self-contained location.

3.1.1 System Accreditation

The most common type of accreditations is a *system accreditation*. A system accreditation is used to accredit a single system, group of similar systems, or local network at a particular location with specified environmental constraints. See **Figure 1**.

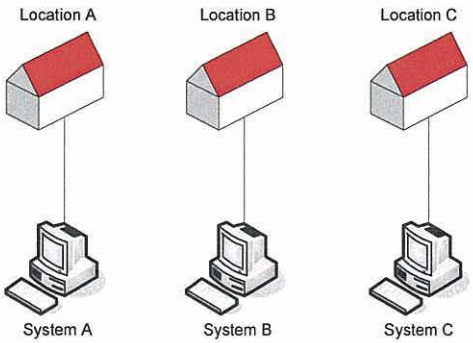


Figure 1 - System Accreditation Model

A system accreditation is warranted when information resources require special security considerations because of the risk and magnitude of the harm resulting from the loss, misuse or unauthorized access to or modification of the information or information resources involved. The certification process assesses all of the relevant security controls, (i.e., management, operational, and technical controls) for the major application or general support system with the resulting accreditation authorizing operation at an agreed upon level of residual risk. A system-accredited system may be transferred to another location, with its certification and accreditation documentation. Applications are evaluated and approved for use upon the system which they operate.

3.1.2 Type Accreditation

In some situations, system or specified set of hardware components is intended for installation at multiple locations. The application or system usually consists of a common set of hardware, software, and firmware. Since it is difficult to accredit a common application or system at all possible locations, the Designated Accrediting Authority (DAA) may issue a *type accreditation* for typical operating environments. Type accreditations are used to certify and accredit multiple instances of system, group of systems, or networking components for operation at approved locations with the same type of computing environment. See **Figure 2**.

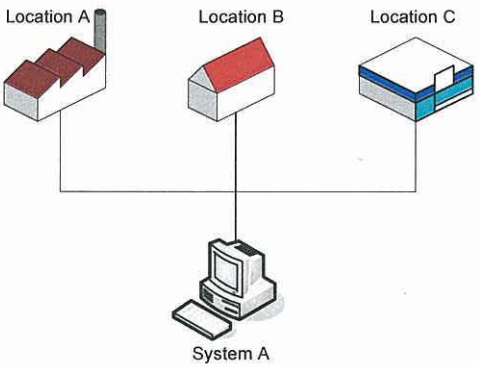


Figure 2 - Type Accreditation Model

The DAA must include a statement of residual risk and clearly define the intended operating environment for the major application or general support system. The DAA must also identify specific uses of the application or system and operational constraints and procedures under which the application or system may operate.

Type accreditations provide an efficient way to accredit systems and network components meeting specified security requirements and employing selected security controls for a single application or system distributed to multiple locations. Type accreditations tend to significantly reduce the field-level assessment activities because the local organization is provided with the initial system documentation needed for accreditation, including specific security operating procedures.

A Type accreditation is a method for accrediting systems or network components that are essentially the same (e.g., alike in function, hardware, software, intended physical environment, operating system and security requirements) but will be fielded to different locations.

The DAA accredits the system or approves applications for use based on their evaluation of all documentation and their level of compliance with implementation guidance, environmental specifications, and testing requirements. Systems distributed over regions, in various state locations, or in remote locations can be organized into a common management approach and accredited together.

Enclaves, once defined, can be Type-accredited.

Groups of laptops or desktops, if configured and managed the same, can be Type-accredited.

With type accreditations, local personnel at the installation site assume responsibility for monitoring the operational environment for compliance with the stated assumptions about the environment and approved configurations as described in the accreditation documentation. Sites must provide security artifacts (i.e., validation of the implementation of the type accreditation) to the DAA for approval.

3.1.3 Site Accreditation

A Site accreditation is a method for accrediting a particular site, and may be optimal given the number of systems, applications or unique operational characteristics. Site accreditation is practical when disparate systems are controlled by a single management authority within a well-defined physical site, e.g., business center, building, or floor. See **Figure 3**. When a type-accredited system or application is integrated into an accredited site, the Type accreditation becomes an appendix to the Site accreditation documentation.

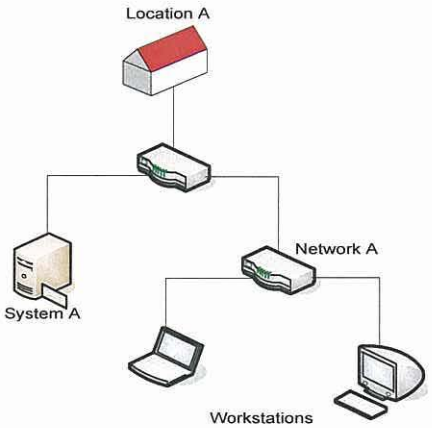


Figure 3 - Site Accreditation Model

The MCCAP applies each of these accreditation types and may be tailored to meet the specific needs of the organization and IT system.

3.2 UNIQUE ACCREDITATIONS

3.2.1 Platform IT

Platform IT is defined as computer resources, both hardware and software, that are physically part of, dedicated to, or essential in real time to the mission performance of special purpose systems such as weapons, training simulators, diagnostic test and maintenance equipment, calibration equipment, equipment used in the research and development of weapons systems, medical technologies, transport vehicles, buildings, and utility distribution systems such as water and electric. As with all other Marine Corps ISs, Platform IT will be accredited through the process described herein and operated within an acceptable level of risk. Platform IT will only be evaluated against those specific system security controls that apply to the IT portion of the platform.

3.2.2 Circuits

The Marine Corps approach to circuit connection approval applies to connections between local systems, networks and applications requiring MCEN services or transport capability, and will standardize connection requirements and ensure an acceptable level of risk is maintained for all systems and networks throughout the Marine Corps.

Circuit connection approval is designed to compliment the Defense Information System Agency's (DISA) NIPRNET and SIPRNET Connection Approval Process (CAP) for the

DoD Information System Network (DISN). The principle purpose of the CAP is to protect and secure the entities comprising the MCEN with a proper balance between the benefits to the operational missions, the risks to those same missions, and the life-cycle costs. The MCEN DAA will consider any systems, networks or applications that have received DISN approval to connect and have undergone DISN CAP validation compliance testing approved for connection to the MCEN. Additionally, systems connecting to the DISN that have undergone the Cross Domain Solution process will also meet MCEN requirements and obtain approval. These connection approvals are contingent on a MCEN DAA review of the DISN CAP approval package.

DoD policy requires certification and accreditation of all ISs prior to operations to ensure a system will maintain the IA and security posture of the GIG. Systems and applications connecting to the MCEN must have undergone and received proper accreditation, e.g. interim or full Authorization to Operate. The accreditation approval for systems, networks and applications requesting connection to MCEN must have documented information identifying and describing the residual risks that will be assumed by the MCEN and accepted by the MCEN DAA. Typically the necessary accreditation is contained in the system or application package[2] developed in accordance with this Directive.

3.2.3 Commercial Connections/Networks

The DoD categorizes commercial connections/networks as outsourced IT-based processes. This is a general term used to refer to outsourced business processes supported by private sector ISs, outsourced information technologies, or outsourced information services.

In one example, Marine Corps Public Affairs would need access through a commercial internet service provider to gain access to public social networks, e.g, MySpace, that have been restricted at the .mil domain. In other examples, naval law enforcement may need access to sites where their military address may draw adverse attention and compromise a particular case. In both examples, the local Marine or Navy unit would need to prepare accreditation documentation to provide evidence the connection was secure.

3.2.4 Wireless Networks

See Marine Corps Enterprise IA Directive 014 for steps to accredit both unclassified and classified wireless networks.

---

[2] See section 3.6

3.3 WHY IS C&A IMPORTANT?

The Certification and Accreditation process ensures adequate security measures are in place to protect the information that resides on Marine Corps systems. This process is applicable to all Marine Corps systems under development and those already in production. In addition, Federal laws and regulations *require* Federal agencies to perform C&A activities at least every 3 years or when a major change has been made to the system. To meet the C&A requirements mandated in Federal laws, the Marine Corps has outlined C&A requirements in this guide. Therefore, organizations, commands, bases and camps within the Marine Corps are required to adhere to Marine Corps-wide policy.

The C&A process achieves the following—

- Validates security requirements established for a system or network
- Examines implemented safeguards to determine if they satisfy Marine Corps' security requirements and identifies any inadequacies
- Obtains management approval to authorize initial or continued operation of the system or network.

3.4 C&A LIFE CYCLE

Certification and Accreditation must be integrated and performed during the IS procurement/development lifecycle processes to ensure that appropriate security controls are in place to facilitate adequate security for the system or application.

Applications, systems, and networks must be properly accredited by the MCEN DAA before they can be operated within the MCEN environment. C&A must be initiated concurrently with system (or change) concept definition. In the case of procured applications or systems, security requirements must be identified and validated before the resource is purchased. Acquisition alone does not guarantee that a system or application can be operated on or connected to the MCEN. By definition, the MCEN is defined as all networks and ISs, in garrison or deployed, wired or wireless, Marine Corps owned or contracted to the Marine Corps that process Marine Corps information.

System security accreditation must be scheduled for completion prior to operational deployment. The balance of the C&A activities and tasks then must be integrated into the system procurement/development life-cycle schedule. A legacy system must enter the C&A process when it is in need of compliance validation or it changes such that its security posture is affected. The C&A process must continue in step with the system acquisition/development life cycle, through post-accreditation and disposal, as outlined in the *Certification and Accreditation Process* section 5.0.

3.5 C&A MAINTENANCE

Automated Information Systems (AIS), sites, and enclaves are dynamic and continuous. System technology and users, data and information in the systems, risks associated with the system and, therefore, security requirements are ever changing. Each command must design, execute, and maintain a Lifecycle Implementation Plan that specifies the C&A schedule for all systems. The plan must include a reevaluation of system security postures at least annually or when there are significant modifications that change the security posture or accreditation status. The DAA may revoke accreditation and connectivity for systems, applications, and networks when it is determined that appropriate IA controls are implemented incorrectly or ineffectively.

3.6 C&A DOCUMENTATION

C&A documentation is required for all IT systems, applications, and networks/sites residing within the MCEN boundaries. Because each system's size, scope, and function are unique, not every accreditation requires identical documentation. The certification documentation in the Application Security Plan (ASP), or DIACAP package must include any unique requirements for each IS to be accredited.

ISs developed or procured by a program office or local authority must be accredited at the system level prior to deployment and identified at the site level as part of an overall site accreditation.

The C&A documentation must be developed at the inception of the application/system's life cycle to specify requirements, establish security controls, guide security actions, maintain operational system security, and document risks, certification level of effort, and other C&A activities.

A key component of DIACAP is automation of the C&A process, with the goal of providing; dynamic data exchange, IA status (metrics) and FISMA reporting, Vulnerability Assessment management, and C&A status tracking. The Marine Corps utilizes the Xacta IA manager to accomplish automation of the MCCAP. All Marine Corps C&A packages will be developed, processed, tracked, and monitored through use of Xacta IA Manager.

3.6.1 DIACAP Package

A DIACAP package is the collection of documents or data objects generated through MCCAP implementation for an IS. A DIACAP package is developed through implementing the activities of the MCCAP 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 connection approval. A DIACAP package,

prepared as described in DoDI 8510.01, is required for systems to be accredited for use in Services other than the Marine Corps.

There are two types of DIACAP packages, the comprehensive package containing all information connected with the certification of the IS, and the executive package containing information for an accreditation decision. The comprehensive package contains, at a minimum, the System Identification Profile (SIP), the DIACAP implementation plan or the ASP, and the Plan of Actions & Milestones (POA&M) if required. The executive package contains, at a minimum, the SIP, and the POA&M if required.

Marine Corps users or Program Managers will start their C&A process by supplying the information in a DIACAP package for systems and sites, or an ASP for applications. See section 5.0 for the C&A process.

When the required C&A tasks have been completed, an accreditation package with all required documentation must be assembled and presented to the MCEN Certifier for review. The required documentation will have been specified in the DIACAP package or ASP. The MCEN Certifier must forward the accreditation package to the MCEN DAA with a recommendation to grant an accreditation decision.

3.6.2 Application Security Plan (ASP)

An ASP is an abbreviated C&A documentation for applications. ASPs are required for applications to be approved for use solely on the MCEN. The ASP is a questionnaire and is appended to the corresponding enclave system DIACAP as Appendix I, Applicable System Development Artifacts. The ASP will be entered in the Xacta IA Manager.

4.0 ROLES AND RESPONSIBILITIES

Central to the C&A process is a clear understanding of the roles and responsibilities of IT system owners, certifying and accrediting officials, IT security staff, and end users. C&A is not just a technical undertaking. At the core of the C&A process is the coordinated effort between all officials involved in the operation of Marine Corps's IT infrastructure.

Within the United States Marine Corps, there are many significant roles in contributing to the secure development and operation of ISs. This Directive allows Marine Corps organizations to adapt the C&A roles into their respective organizational management structure to best manage the risks to the mission throughout the information technology system life cycle: system development, operation, maintenance, and disposal.

4.1 HEADQUARTERS MARINE CORPS C4 CIO

Headquarters Marine Corps C4 CIO shall:

- Appoint a Marine Corps Senior IA Official (SIAO) in accordance with Reference (a) to direct and coordinate the Marine Corps IA Program consistent with the strategy and direction of the Defense-wide Information Assurance Program (DIAP).
- Ensure that implementation and validation of IA controls through the MCCAP is incorporated as an element of Marine Corps IS life cycle management processes.
- Ensure that the MCCAP status of Marine Corps ISs is visible to the DoD and DON CIOs.
- Ensure collaboration and cooperation between the MCIAP and DAA structure.
- Ensure a program or system manager is identified for each Marine Corps IS.
- Establish and manage a MCCAP Plan of Actions and Milestones (POA&M) program.
- The SIAO is senior to the DAA.

4.2 SENIOR IA OFFICIAL (SIAO)

The Marine Corps SIAO is appointed by the Marine Corps CIO. This position is the responsibility of the Director, Information Assurance Division, (HQMC C4 IA). Under the authority, direction, and control of HQMC C4, and in accordance with DoDI 8510.01, the Marine Corps SIAO shall:

- Track the C&A status of ISs that are governed by the MCIAP.
- Ensure the IA controls assigned to each information technology governed by the MCIAP address the assurance of the enterprise information environment (EIE).
- Establish and manage a coordinated IA certification process for ISs governed by the MCIAP. This includes but is not limited to:
    - Functioning as the Certifying Authority (CA) for all governed ISs or delegating the duties as needed.
    - Ensuring and overseeing a qualified certification cadre (e.g., validators, analysts, CA representatives).
    - Formally delegating CA representatives as necessary.
    - Establish and enforce the C&A process, roles and responsibilities, and review and approval thresholds and milestones within the MCIAP.

- Serve as the single IA coordination point for Joint or Defense Programs that are deploying ISs to Marine Corps enclaves.

4.3 DESIGNATED ACCREDITING AUTHORITY (DAA)

The DAA is a senior management official or executive with the authority to formally approve the operation of an IT system at an acceptable level of risk. Through accreditation, the DAA assumes responsibility for the risks of operation of the system in a specific environment. The DAA is an executive with the authority and ability to evaluate the mission and business case for the system in view of the security risks. The DAA must have the authority to oversee information technology system mission or business operations of systems under his/her purview. The DAA also approves security requirements documents, memorandums of agreement (MOA), memorandums of understanding (MOU), and any deviations from security policies. In addition to having the authority to approve systems for operation, the DAA has the authority to disapprove systems for operation and, if the systems are already operational, the authority to halt operations if unacceptable security risks exist.

Based on the information available in the final DIACAP package the DAA can make a risk-based decision to:

- grant system accreditation, Authorization to Operate (ATO),
- grant an interim approval to operate the system, Interim Authorization to Operate (IATO),
- grant an interim approval to test the system, Interim Authorization to Test (IATT),
- grant approval to connect the system to a network, Authorization to Connect (ATC), or
- deny system accreditation because the risks to the system are not at an acceptable level, Denial of Authorization to Operate (DATO).

The accreditation decision is documented in the final *accreditation package*, which consists of the accreditation letter and supporting documentation and rationale for the accreditation decision. In some situations, IT systems accreditation may involve multiple DAAs. If so, agreements must be established among the responsible DAAs and the agreements should be documented in the accreditation package. In most cases, it is advantageous to agree to a lead DAA who represents the other DAAs during the C&A process.

The DAA position is designated a special-sensitive position. The DAA must be eligible for a security clearance and access commensurate with all ISs under the DAA's jurisdiction per DoDI 8500.2 table E3.T1 and SECNAV M-5510.30.

Every DAA must be a U.S. Citizen and DoD employee of the pay grade O-6/GS-15 or greater per DoDD 8500.1 and CJCSM 6510.01 except by prior coordination with and authorization from DON Deputy CIO (Marine Corps). For Deployed DAA, as defined below, the seniority is waived for commanders of DON organizations below the pay grade of O-6.

The Marine Corps has one service operational DAA, called the Marine Corps Enterprise Network (MCEN) DAA, residing at Headquarters Marine Corps and developmental DAAs residing at Marine Corps Systems Command (MARCORSYSCOM) and Marine Corps Tactical Systems Support Activity (MCTSSA). Both roles are described below. The Marine Corps also recognizes the role of deployed DAAs. For SCI specific responsibilities, refer to Director of Central Intelligence Directive (DCID) 6/3 paragraph 2.B.5 and Joint DoD Intelligence Information Systems (DoDIIS) Cryptologic SCI Information Systems Security Standards (JDCSISSS) paragraph 1.5.3.

4.3.1 MCEN DAA

The Director, Command, Control, Communications, and Computers Department, Headquarters, US Marine Corps (HQMC C4) is the DAA for all Marine Corps systems. However, the Director has formally designated the Director, Information Assurance Division (HQMC C4 IA) within the C4 Department to function as the DAA for Marine Corps ISs and networks and as the Connection Approval Authority for systems connecting to and from United States Marine Corps resources of the Marine Corps Enterprise Network (MCEN).

The MCEN DAA reports directly to HQMC C4 and holds authority over all MCEN enclaves – NIPRNET, SIPRNET, and the USMC Navy/Marine Corps Intranet (NMCI) Community of Interest (COI) – and must accredit each system, application, or network before it can be operated within the MCEN environment. Systems and applications not properly accredited by the MCEN DAA will be denied access to the MCEN.

4.3.2 MCEN DAA Responsibilities

The responsibilities of the MCEN DAA include:

- Signing operational accreditation documents.
- Granting full accreditation to Marine Corps IT systems. Authorization to Operate (ATO) is based upon the DIACAP team's (validator, certifying authority representative, and MCEN Certifier) comprehensive evaluation of the technical and non technical security features of an IT system or network and the MCEN DAA's acceptance of residual risks and mitigation strategies to maintain an acceptable level of risk to operational (production) naval networks.

- Denying an accreditation because risks to the IT system are not mitigated to an acceptable level. Operational risk is balanced with mission need and the cost of securing the system or reducing the risk.
- Issue written authorization for connectivity and use of operational applications, systems, and networks. This authority to operate includes all operational non-SCI and non-SIOP systems, stand alone systems, business applications or services procured under CMP/PORs and non-CMP/PORs, major applications, and local, base or wide area networks, including those used in support of operational exercises.
- Approves all requests or connection of any operational system or network, regardless of the duration, to any operational enterprise network (e.g., Defense Research and Engineering Network (DREN), NIPRNET, SIPRNET).

In addition to the responsibilities established in MCO 5239.2, the MCEN DAA shall:

- Ensure each Marine Corps IS complies with applicable DoD baseline IA controls and ensure a Plan of Actions and Milestones (POA&M) is in place after receiving a formal recommendation by the MCEN CA representative in order to interconnect with the GIG.
- Ensure assigned systems have appropriate data management and sharing policies and implement security requirements for classified and controlled unclassified information, including establishing security classification guides according to DoD Regulation 5200.1-R.
- Ensure that appropriate access policies are established for all information being produced by the assigned ISs, and that the established roles and privileges are consistent with defined enterprise roles and privileges.
- Authorize or deny testing or operation of assigned Marine Corps ISs.
- Satisfy all responsibilities and training outlined in DoD 8570.1-M, DoDD 8500.1, DoDI 8500.2 and CJCSM 6510.01.
- Execute appropriate requirements for acquisition management listed in SECNAVINST 5239.3A. CMP/POR systems or locally acquired IT assets will be approved for transition to Milestone C and accredited by the MCEN DAA prior to transition to, or operational use on the MCEN.

4.3.3 Marine Corps Developmental DAA (DDAA)

The DDAA is the official responsible for ensuring completion of DAA functions of C&A for applications or systems during acquisition, development, Security Validation and risk mitigation prior to deployment within the operational Marine Corps enterprise. The position is in MARCORSYSCOM, Systems Engineering, Interoperability, Architecture, and Technology (SIAT), Information Assurance & Joint Requirements office.

When a CMP/POR system is ready for installation within the MCEN operational environment, the DDAA, acting as the CA representative for the CMP/POR, performs a risk assessment based on C&A documentation and forwards the C&A package to the MCEN Certifier along with a formal recommendation for accreditation. This process occurs prior to Milestone C. Accrediting responsibility then transitions from the DDAA to the MCEN DAA. **Figure 4** shows the relationship between DIACAP activities and the acquisition cycle

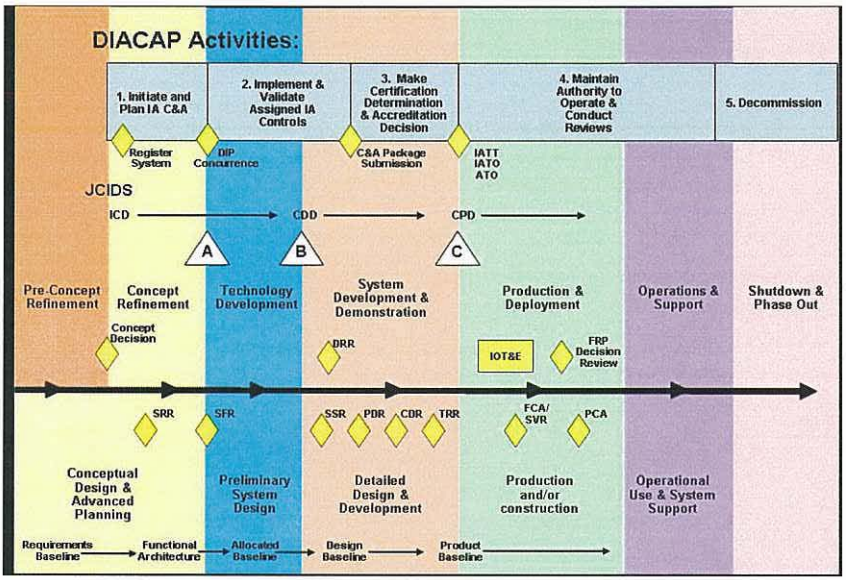


Figure 4 - DIACAP Activities Mapped to Acquisition Cycle

While performing the DAA role in the acquisition community (e.g. for a SYSCOM, developmental activity, or CMP/POR), the DDAA will:

- Ensure planned IA controls for systems that will operate within the MCEN are consistent with IA controls as required by DoDI 8500.2, as mandated by MC Enterprise IA Directives, and as required by the MCEN DAA.
- Issues an Interim Authorization to Test (IATT) on testing networks, training networks and accepts the risks associated with these systems during the testing phase.
- For all ISs, ensure IA controls are implemented and tested.
- Directs and ensures Program Managers/Project Officers developing or acquiring networks, networked systems, independent systems or network components to meet DoD, DON, and Marine Corps IA security requirements.

- Ensures a completed and successful Security validation is accomplished before Milestone C is reached, and provides a formal accreditation recommendation to the MCEN DAA as a CA representative for CMP/POR. DDAA responsibilities for the system do not end until a successful validation is completed and a formal system hand off to the MCEN Certifier is accomplished.

4.3.4 Deployed DAA

The senior commander, commanding officer or officer-in-charge is authorized to perform a limited set of DAA functions when operating while deployed or at sea, and ensures that system and network capabilities are maintained to meet operational mission requirements. This authority shall not be used to circumvent normal configuration control processes and should only be used in mission essential operational circumstances. Units deploying networks and ISs in support of an exercise must have the architecture accredited by the MCEN DAA. Deployed DAAs are responsible to return the application, system, or network to its accredited configuration once the ship, unit, or command returns to port or garrison. Additionally, the Deployed DAA is responsible to inform the MCEN DAA via message or e-mail of all changes made to the security posture of the application, system, or network in order to identify required changes in accredited configurations that affect operational capability.

Marine Corps Deployed DAAs, report to the MCEN DAA concerning issues affecting the network/systems' IA posture.

The Deployed DAA's responsibilities include:

- Signing operational accreditation documents for Marine Corps systems in a deployed environment.
- Granting full accreditation to Marine Corps IT systems in a deployed environment. Authorization to Operate (ATO) is based upon a certification authority representative comprehensive evaluation of the technical and non-technical security features of an IT system or network and the Deployed DAA's acceptance of residual risks and mitigation strategies to maintain an acceptable level of risk to operational (production) naval networks.
- Denying an accreditation because risks to the IT system are not mitigated to an acceptable level. Operational risk is balanced with mission need and the cost of securing the system or reducing the risk.

In addition to the responsibilities established in MCO 5239.2, the Deployed DAA shall:

- While deployed, ensure each Marine Corps IS complies with applicable DoD baseline IA controls and ensure a Plans of Actions and Milestones (POA&M) are in place in order to interconnect with the GIG.

- Ensure assigned systems have appropriate data management and sharing policies and implement security requirements for classified and controlled unclassified information, including establishing security classification guides according to DoD Regulation 5200.1-R.
- Ensure that appropriate access policies are established for all information being produced by the assigned ISs, and that the established roles and privileges are consistent with defined enterprise roles and privileges.
- Satisfy all responsibilities and training outlined in DoD 8570.1-M, DoDD 8500.1, DoDI 8500.2 and CJCSM 6510.01.

4.3.5 Multiple Accreditors

Often different components of a system fall within separate Service or DoD organizational jurisdictions. In order to accredit systems that meet this criterion, the authorities from each jurisdiction must take action to collectively accredit the system. Generally systems in these environments are divided into two types:

- Systems identified at their inception as requiring mutual accreditation
- Systems composed of the interconnection of separately-accredited systems.

Written agreements are required when ISs interconnect, for example, within the Marine Corps, with other Services or agencies, or with government contractors. When separately-accredited ISs managed by different DAAs are interconnected, the DAAs must negotiate the interconnection requirements. A Memorandum of Agreement (MOA) must document the results of the DAA's accreditation negotiations and forms an agreement between or among the participating DAAs.

When a system requires accreditation by multiple DAAs, the roles and responsibilities of the DAAs, certifiers, and other key security personnel of all participating organizations must be clearly defined and documented in the appropriate accreditation documentation.

4.4 CERTIFYING AUTHORITY

The Certifying Authority (CA) provides the technical expertise to conduct the certification throughout the system's life cycle based on the security requirements documented in the DIACAP Package. The CA determines the level of residual risk and makes an accreditation recommendation to the DAA.

The CA is the official responsible for performing an independent, comprehensive evaluation of the application's and/or system's compliance with security features and safeguards with respect to the security requirements (IA controls) stated in DoDI 8500.2 and other applicable DoD and DON requirements.

4.4.1 Certifying Authority Responsibilities

The CA is responsible for making a technical judgment for system compliance with applicable DoD/DON security requirements, identifying and assessing the risks associated with operating the system, coordinating the certification activities, and issuing a certification/risk recommendation for the system to the DAA for consideration in an accreditation decision. The duties of the certifying authority include:

- Coordination of certification activities with the PM and validation team;
- Signing the system's C&A documentation along with the DAA, PM and User Representative (UR) indicating agreement with the system's architecture, security features and C&A plan;
- Determining whether a system is ready for certification.
- Conducting the certification process by performing a comprehensive evaluation of the technical and non-technical security features of a system. This includes providing assurance that vendor products used by the IT systems have been certified and accredited, and vendors who develop, house, or are otherwise involved with Marine Corps systems are subject to the same or higher standards followed by the United States Marine Corps.
- Reporting the status of certification and recommending to the DAA whether or not to accredit a system based on documented residual risk
- Certify systems under their cognizance and sign the certification documents as the Certification Official and issuing a recommendation to the DAA that includes an assessment of risk of operating the application and/or system. The recommendation may be: issue Denial of Authorization to Operate (DATO), issue IATO, issue ATO, or issue Interim Authorization to Test (IATT). The CA's recommendation to the DAA is required for all applications, system and networks.

4.4.2 Certifying Authority Representatives

The Marine Corps SIAO assigns the MARCORSYSCOM SIAT IA Team Representative Information Assurance & Joint Requirements director as the Certifying Authority representative for Marine Corps CMP/POR, called the SYSCOM Certifier. The SYSCOM Certifier provides recommendations to the MCEN DAA for networks and ISs moving from acquisition to operational status. The SYSCOM Certifier may assign certifier responsibilities to external systems commands, e.g., SPAWAR, for programs acquired and developed by those external organizations. However, those so assigned must still submit their recommendations through the SYSCOM Certifier for Marine Corps

The Marine Corps SIAO assigns the Head, System Security Branch, IA Division, HQMC C4 as the Certifying Authority representative for the MCEN, called the MCEN Certifier. Certification recommendations to the MCEN DAA for networks and ISs that are operational within the MCEN are provided by the MCEN Certifier.

The Marine Corps local IA authority, normally the G-6 at the Marine Corps Installations regions, Major Subordinate Commands and Marine Corps Bases are appointed as Certifying Authority representatives for the networks, systems, and information technology components under their responsibility. They are to consult with the MCEN DAA to ensure secure system operation within the identified constraints and in compliance with applicable IA policies and procedures.

These CA representatives are officials acting on behalf of the CA. Their responsibilities include the following:

- Ensure that the Common Criteria requirements for IA and IA-enabled products are identified and documented prior to contract negotiations.
- Evaluate the system's robustness requirements and mission and customer needs and recommend a specific Evaluation Assurance Level (EAL) for a particular product to the MCEN DAA.
- Test, validate, and document the product's ability to meet the EAL.
- Provide the MCEN DAA with sufficient information to make a risk determination about a non-NIAP-evaluated product.
- Identify and document product security requirements that were unmet or non-compliant.
- Develop and execute component-level tests to assess the risk of unmet security requirements to assist the MCEN DAA in determining the IS's overall risk of compromise.
- Ensure that all IA and IA-enabled IT products are configured in accordance with DISA and/or NSA Security Technical Implementation Guidelines (STIGs) and Security Recommendation Guides (SRGs) as directed by the DAA.
- Review all changes to the MCEN for IA impact.
- Ensure that the Contracting Officer incorporates into the contract requirements based on the Mission Assurance Category (MAC), security classification, sensitivity, and need-to-know of information and ISs in accordance with reference (b), the permissible uses of information and associated mission or business rules of use, and the distinction between information that is operationally sensitive and information that can be made available to the public.

- With the MCEN DAA, ensure that system security requirements are identified, resourced, and implemented to provide an acceptable level of risk. For networks and systems in the acquisition process, the SYSCOM Certifier has the lead. For operational networks and systems, the MCEN Certifier has the lead.
- With the MCEN DAA, ensure that appropriate IA resources are identified and acquired during the initial C&A Phase. The SYSCOM Certifier has the lead.
- State any unique requirements for each IS to be accredited in the certification documentation.
- Continuously assess and guide the quality and completeness of C&A activities and tasks and the resulting artifacts.
- Coordinate security requirements with the MCEN DAA, the PM, and the UR. For networks and systems in the acquisition process, the SYSCOM Certifier has the lead. For operational networks and systems, the MCEN Certifier has the lead.
- Coordinate with the UR, MCEN DAA and PM on determining the MAC and Confidentiality Level (CL) of developing systems, in addition to the proper certification levels. For networks and systems in the acquisition process, the SYSCOM Certifier has the lead. For operational networks and systems, the MCEN Certifier has the lead.

4.4.3 Validator

The Validator is responsible for the validation of applicable IA Controls for an assigned Marine Corps system, including the development of appropriate test procedures, execution of test procedures and the accurate documentation of system security posture based on the results of security testing. The SIAO appointed the MCEN C&A team leader located at the MCNOSC as the MCEN Validator.

The Validator develops the DIACAP Scorecard and Validation Report for the assigned system(s) and facilitates the coordination of the PM, UR, Certifying Authority Representative and MCEN DAA agreement of the documentation.

The Validator's critical function is to examine through demonstration, inspection, and/or analysis the extent to which an IT system meets a set of specified security requirements (as specified by the DAA and governing instructions and directives). The requirements focus centers on deploying effective countermeasures that satisfy the IA objectives of sufficient confidentiality, integrity, availability, and accountability. The appropriate Certifying Authority approves the evaluation efforts completed by the Validator.

The Validator provides technical expertise to the Certifying Authority or PM and facilitates interaction between the program office and the Certifying Authority. The program office provides the validator with the DIACAP Implementation Plan (DIP) and basic system information (mission need statement, schedule, performance, system architecture, CONOPS, etc.) to ensure the DIACAP Package is accurate.

The validator provides independent verification and validation of the system's security controls and safeguards designed through the security engineering process. Security engineering is the term given to the various processes used in developing the security controls and safeguards of the IT system. These ensure the necessary protection assurance for equipment, data, information, applications, and facilities to meet security policy/requirements. A conflict of interest exists when the same personnel fulfilling the security engineering function also assesses the IT system.

4.5 PROGRAM MANAGER

The Program Manager (PM) represents the interests of the system throughout its life cycle (acquisition or maintenance, life cycle schedules, funding responsibility, system operation, system performance, and maintenance). The organization that the PM represents is determined by the organization that has been assigned life cycle management of the system and must appropriate funds to support IA standards

The PM coordinates all aspects of the system from initial concept, through development, to implementation and system maintenance. The DAA, CA, Validator, and UR provide advice, information, and guidance to the PM throughout the C&A process.

The PM is responsible for the system throughout the life cycle (cost, schedule, and performance of the system development). The PM's function is to ensure that the security requirements are integrated in a way that will result in an acceptable level of risk to the operational infrastructure as documented in the DIACAP Package. The PM keeps all participants informed of life cycle actions, security requirements, and documented user needs.

The PM's responsibilities include the following:

- Coordinate with the DIACAP team to ensure that system security requirements are identified, resourced, and implemented to provide an acceptable level of risk.
- Work with the DIACAP team to ensure that IA resources are identified and acquired during system analysis and design for formal completion of DIACAP Activity I.
- Account for credible cost, schedule, and performance reporting.

- Coordinate with the Information Systems Security Engineer (ISSE)/Information Assurance Manager (IAM) to ensure that IA requirements are identified and built in to new software releases.
- Ensure that IAVAs are implemented and managed in accordance with DoD, DON, and Marine Corps policies and procedures.
- Provide systems that interoperate and integrate IA solutions that adhere to the MCEN architecture, enable network-centric warfare, and conform to the defense-in-depth model.
- Ensure that IT-related contracts specify that vendor products require National Information Assurance Partnership (NIAP) evaluation.
- Monitor the IS throughout the system's life cycle for changes in IA control compliance. This occurs continuously from installation until the system decommission. Any change in the life cycle and accreditation status of the system and environment will be evaluated to determine if further action is required.
- Conduct Annual Reviews of assigned IA controls on the program/system's yearly anniversary.

4.6 IA MANAGERS/OFFICERS (IAM/IAO) AND INFORMATION SYSTEM SECURITY ENGINEER (ISSE),

The United States Marine Corps has positional functions that are responsible for the IA posture and policy implementation for Marine Corps systems. The Information Assurance Manager (IAM) is the individual responsible to the DAA for the Information Assurance Program of Marine Corps ISs within a particular organization. The Information Assurance Officer (IAO) is responsible to the IAM for ensuring that the appropriate operational IA posture is maintained for a specific DoD IS or organization. The ISSE is responsible for ensuring that the IT system's information protection requirements are satisfied.

4.6.1 IA Manager (IAM)

The IAM is appointed by the Certifying Authority representative and is responsible for the IA program of a DoD IS or organization, and ensuring compliance to the Marine Corps IA Program. The IAM is an integral part of the C&A process. An IAM may be assigned to support a PM to deliver a Program of Record (POR) with IA integrated throughout the system development lifecycle, or assigned to a command to perform the day-to-day system security oversight responsibilities, including C&A of operational networks and systems. The IAM's responsibilities include the following:

- Act as the primary IA technical advisor to the MCEN DAA and formally notify the MCEN DAA of any system or architecture changes that affect the Marine Corps IA posture.
- Develop and maintain a command-level IA program in accordance with references (a) and (b) that identifies IA architecture, requirements, objectives, policies, personnel, processes, and procedures.
- Ensure that IA officers and privileged users are appointed in writing and provide oversight to ensure that they are following established IA policies and procedures.
- Ensure that information ownership responsibilities are established for each Marine Corps IS to include accountability, access approvals, and special handling requirements.
- Ensure that IA certification documentation is developed and maintained according to current DoD C&A guidance by evaluating, reviewing, and endorsing such documentation and recommending action to their CA representative.
- Review and endorse all IS accreditation or certification support documentation packages.
- Maintain a repository for all C&A documentation and modifications pertaining to all Marine Corps IT assets within the IAM's purview.
- Ensure that all newly-appointed IAOs and privileged users meet all qualifications.
- Ensure all users on the MCEN receive annual IA Awareness training.
- Ensure that all newly-appointed IAOs and privileged users are U.S. citizens. Foreign nationals who are direct or indirect hires and are currently appointed as an IAO or privileged user may continue in these positions provided they satisfy the provisions of DoDD 8500.1, *Information Assurance (IA)*, and DoDI 8500.2, *Information Assurance (IA) Implementation* are under the supervision of an IAM who is a U.S. citizen; and are approved in writing by the DAA.
- When circumstances warrant, a single individual who is a U.S. citizen may fill both the IAM and IAO roles. These exception circumstances shall be tightly controlled and limited. These circumstances must be noted on the appointment letter along with justification of the circumstance clearly defending the need for the deviation from desired norms (dual roles as IAO and IAM).
- Ensure that all IAOs and privileged users receive the necessary technical and IA training, education, and certification to carry out their duties.

- Ensure that IA inspections, tests, and reviews are coordinated with the MCEN DAA and local security managers, when applicable.
- Ensure that the IT system is registered and entered into the Xacta IA Manager database in order to initiate the C&A process.
- Ensure that all management review items are tracked and reported to HQMC C4, Marine Corps Network Operations and Security Command (MCNOSC), and MARCORSYSCOM.
- Ensure that security events are properly investigated and incidents reported to the MCEN DAA. In addition, the IAM shall ensure that responses to IA-related alerts are coordinated and reported.
- Complete the MCCAP prior to connecting to other networks under the control of a different DAA.
- Coordinate with the Personnel and Physical Security Officers to ensure that physical and personnel access controls for Marine Corps-owned facilities including ISs, comply with established policies and procedures.
- Oversee system DIACAP Implementation Plans (DIP) to ensure that MCEN DAA-directed IA policies and procedures are implemented and functioning as described.
- Ensure that all sensitive and classified data is destroyed in accordance with DoD, DON, and Marine Corps policies.
- Coordinate on local security policies and procedures with security managers as required to comply with DoD, DON, and Marine Corps IA policies and directives.
- Use the MCEN DAA-prescribed methodology and tools to conduct risk assessments of Marine Corps ISs.

4.6.2 IA Officer (IAO)

The IAO is appointed by the IAM. The IAO's responsibilities include the following:

- Comply with all access requirements specified in reference (a).
- Coordinate local system security with local security policies and procedures as required, complying with DoD, DON, and Marine Corps IA policies and directives.
- Assist the IAM in performing the duties and responsibilities outlined above.
- Ensure that enclaves, sites, systems, and AISs are certified and accredited.

- Ensure that accreditation and/or certification support documentation packages for system(s) for which the IAO is responsible are developed, maintained, and updated as required.

- Ensure that all Marine Corps system IA-related processes are monitored and accessible to properly-authorized individuals approved by the MCEN DAA.

- Ensure that all users have the requisite security clearances and need-to-know and are aware of their responsibilities before granting them access to a Marine Corps IS.

- Ensure that all IT users and operators read, understand, and sign the appropriate System Authorization Access Request (SAAR) (i.e., NIPRNET, SIPRNET, JWICS, etc.) prior to receiving access to IT resources. See MCEN Directive 007, Resource Access Guide for an example of an approved SAAR form.

- Ensure that IA and IA-enabled software, hardware, and firmware comply with the appropriate MCEN DAA-approved security configurations.

- Coordinate security procedures with the IAM and security managers, initiate investigative procedures for security events, and institute protective or corrective measures when an IA incident or vulnerability is discovered.

- When investigative procedures must be conducted by law enforcement or Inspector General personnel, ensure the integrity of the investigation, prevent the loss or alteration of any data potentially involved in the investigation, and keep the IAM and all other appropriate persons informed throughout the duration of the investigation.

- Ensure that Marine Corps IS back-up and recovery processes are developed, tested (initially and annually thereafter), and documented in the C&A package.

- Coordinate with IT personnel to develop and test the local IA Contingency Plan and Disaster Recovery Plan, which are part of the overall Continuity of Operations Plans (COOP), to ensure confidentiality, integrity, availability, and recoverability of critical ISs and data is achieved during and after a disaster. Additionally, coordinate with the appropriate representatives to ensure that the Contingency and Disaster Recovery Plans meet command objectives and are tested prior to system operation and annually thereafter.

- Coordinate all IA-related issues that call for local execution of contingency plans with the IAM, IT personnel, and security managers, as required.

4.6.3 Information Systems Security Engineering (ISSE)

The ISSE's responsibilities include the following:

- Coordinate with the PM to ensure that all information protection requirements for the IS are identified.
- Ensure that all information protection requirements have been integration into IT acquisition processes through purposeful security design or configuration and built in to new IT system releases.
- Coordinate with the System Engineer to ensure that the customer's information protection needs are satisfied.
- Provide evidence and documentation from the ISSE process to ensure that the DIACAP Package meets the information protection requirements for the certification level appropriate for the criticality and the complexity of the IT system.
- Ensure that the security controls meet or exceed the information protection requirements by conducting information protection effectiveness tests at the end of each stage of the ISSE process.
- Provide Contingency and Disaster Recovery plans for developed or acquired networked systems and networks before production and fielding that apply to the unique features of those capabilities.

4.7 COMMANDERS

Commanders of Marine Corps organizations receiving network services must ensure IA controls are in place at their command as well as on the provided networks. Physical control of spaces and annual IA awareness training for all command personnel are two examples of controls that are the responsibility of the command receiving network services and affect accreditation of the network services received.

Commanders of Marine Corps organizations providing system or network services, either connected to the backbone or part of a local sub-enclave, whether contracted or performed by government employees, must ensure IA controls are in place for those systems or networks and must only provide network services to commands that have an active IA program and meet service MCEN DAA's conditions for operation.

Command mission and role in supporting and providing IS services greatly affects the scope of responsibilities for IA Workforce personnel. When choosing command IA workforce personnel, the following apply:

- All IA workforce personnel are assigned in writing, have a statement of responsibilities, are trained, and are certified per DoDI 8500.2 and DoD 8570.1-M.
- All personnel with privileged access will sign the Privileged Access Agreement and Acknowledgement of Responsibilities found in Appendix 4 of DoD 8570.1-M.
- Maintain appropriate separation of duties between management and technical positions. The Information Assurance Officer (IAO) and System Administrator (SA) positions should be filled separately except for extreme operational constraints. This separation of technical and management positions impacts the acceptable level of risk to operations.

4.8 USER REPRESENTATIVES (UR)

The UR represents the operational interests of the user community and ensures the IT system meets the user needs. The UR must review the C&A documentation for compliance with the Mission Needs Statement or Initial Operational Capability Statement, and for concurrence with the security features of the system. The UR has the responsibility for ensuring that the appropriate IA controls have been identified, assigned, and validated so that the implementation of the IA controls meet user community needs. The UR will identify and document any IA controls that interfere with the mission execution.

5.0 MARINE CORPS C&A PROCESS (MCCAP)

This section describes the MCCAP for identifying, implementing, validating, certifying, and managing IA capabilities and services, expressed as IA controls, and authorizing the operation of ISs in accordance with OMB Circular A-130 Appendix III, FISMA, DoDI 8510.01 and other Federal requirements.

DoD has defined the C&A process as a series of ongoing events (Figure 5). This is a valuable strategic view of the C&A process. However, a day-to-day task process is required to help the Marine submitting the documentation understand what specific steps need done to assure that the accreditation decision can be reached in a timely manner.

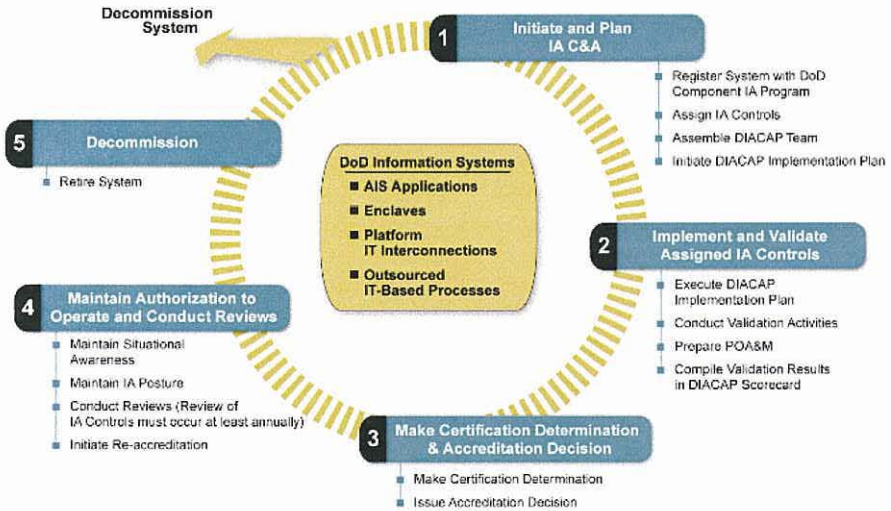


Figure 5 - DoD C&A Process Cycle

Taking into account FISMA requirements, particularly in light of evolving DoD standards on C&A, the Marine Corps has established the Marine Corps C&A Process (MCCAP) to assure that each task identified in the C&A process is addressed according to Marine Corps requirements. The MCCAP facilitates the immediate response to changes in IT, the way the Marine Corps acquires, operates, and uses information technology, and to comply with emerging Federal requirements and guidelines. The MCCAP provides a quick, focused assessment of Marine Corps systems and networks with regards to preparing for or in progress towards full accreditation. As a result, Marine Corps IT assets, information, and resources, provides appropriate levels of

protection. In order to facilitate the process of obtaining the authorization to operate, the MCCAP should commence at the inception of the system's development life cycle.

There must be a clear process identified where the work done can be rolled into the required tasks (and subtasks) outlined in this guide, drawn from DoD Instruction 8500.2, *Information Assurance (IA) Implementation* (DoDI 8500.2), *DoD Information Assurance Certification and Accreditation Process (DIACAP)* (DoDI 8510.01), the DIACAP Knowledge Service, and from NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems* (NIST SP 800-37). This section establishes and implements a common approach for specific tasks and subtasks required to complete the Certification and Accreditation of an information technology system, in accordance with OMB Circular A-130, Appendix III, compliant with the Department of Defense and federal law.

Within the MCCAP, there are five major components that assure a full system security review in order to comply with DoD C&A standards, and ensure complete and viable documentation. They are:

- Initiate and Plan IA C&A
- Implement and Validate Assigned IA Controls
- Make Certification Determination and Accreditation Decision
- Maintain Authority to Operate and Conduct Reviews
- Decommission

See **Figure 6**, which diagrams this methodology.

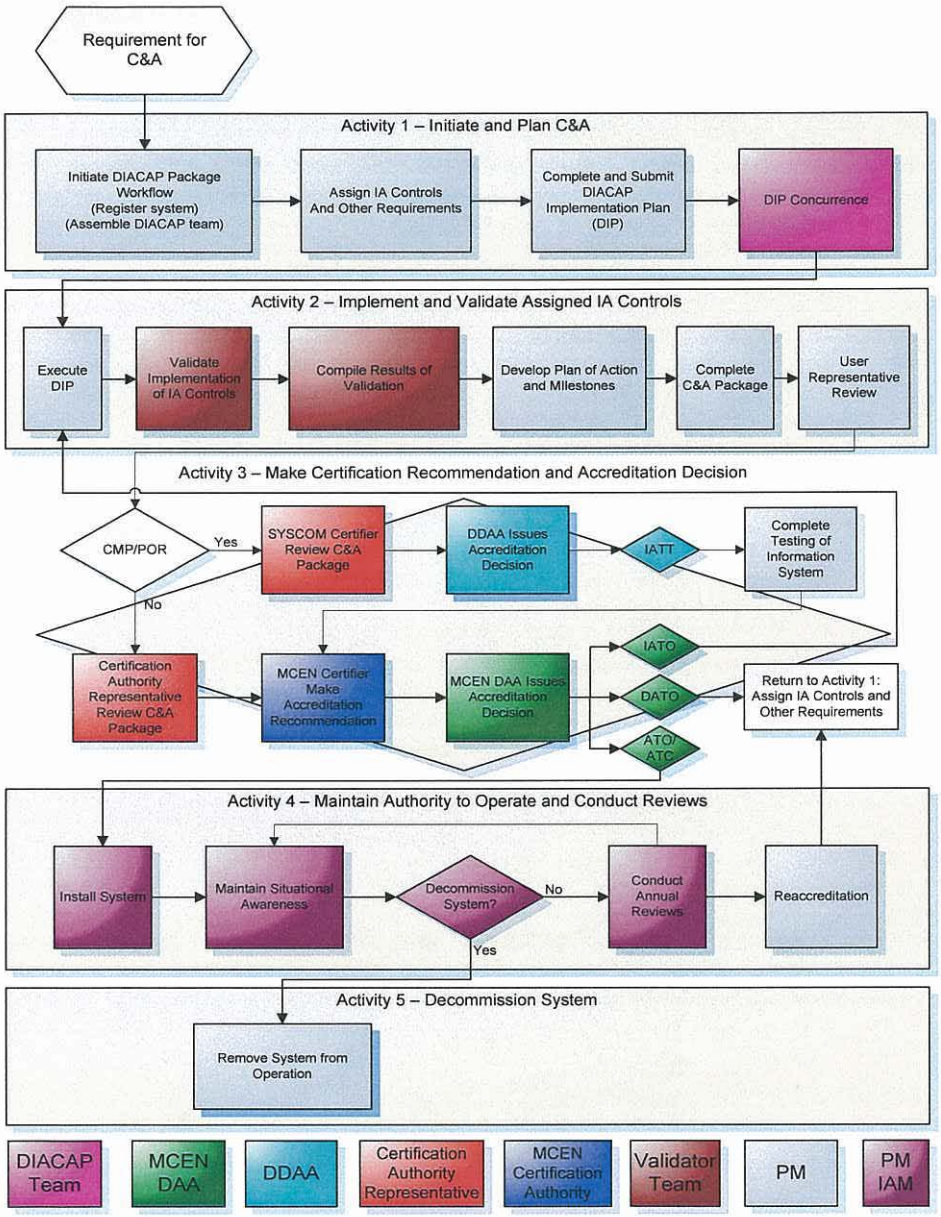


Figure 6 - Marine Corps C&A Process Diagram

The MCEN DAA considers the applications/systems associated with each enclave to be artifacts of their respective enclave. Consequently, there is a DIACAP Package for each of the three MCEN enclaves, and, in most cases, C&A documentation for individual applications and systems is prepared in an abbreviated form as an appendix to the associated system or enclave DIACAP Package[3].

When applications and data owned by one Marine Corps organization are hosted on a system or transact data across a system network owned by another organization, certification and accreditation activities must be coordinated between that organization and the MCEN DAA. The system owner is responsible for taking the lead on coordination and for funding the C&A activities.

Requests for accreditation come either from organizations within or external to the Marine Corps. Requests originating within the Marine Corps come either from MARCORSYSCOM or outside MARCORSYSCOM. If the submission is from the operating forces or subordinate command within the Marine Corps, the documentation also shall include the operating force or subordinate command Certifying Authority representative certification statement.

[3] See Section 3.6.1

5.1 INITIATE AND PLAN IA C&A

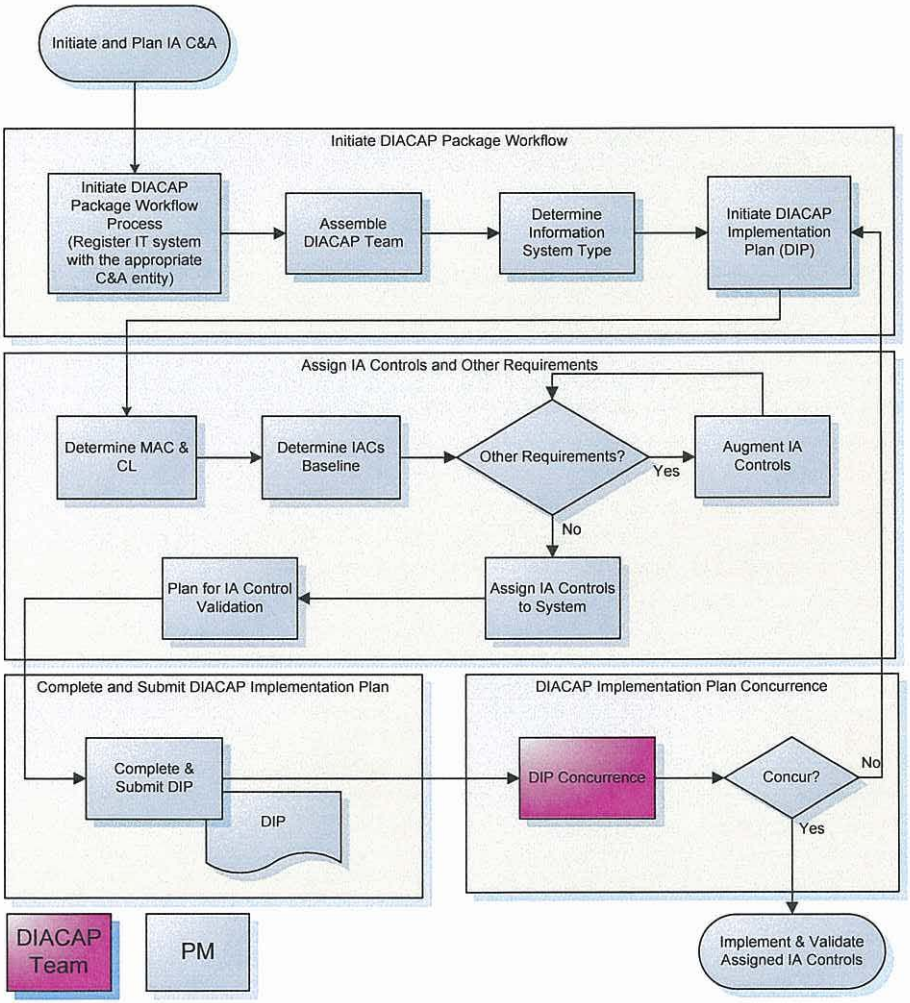


Figure 7 - Initiate DIACAP Package Workflow

The request for System Certification and Accreditation process begins with the initiation and planning of the C&A effort which encompasses the development and submission of a DIACAP package[4] to the MARCORSYSCOM C4II IA Division (for

[4] See section 3.6.1

Programs of Record and Joint systems) and to MCEN C&A for all other ISs, networks, and circuits. To assure a quick and timely assessment of the system, this documentation must contain complete information concerning the IT system. The Initial Assessment effort allows customers[5] to "jump-start" the C&A process, to quickly determine their security status, gather appropriate information, and determine what changes have to be made to bring them into compliance with United States Marine Corps and other Federal regulations. The Initial Assessment is comprised of four primary tasks illustrated in **Figure 7**:

- Initiate DIACAP package workflow,
- Assign IA controls and other requirements,
- Complete and submit DIACAP implementation plan, and
- Obtain DIACAP implementation concurrence.

Each of the tasks contains a series of subtasks that help to facilitate the MCCAP. These tasks are described as follows:

5.1.1 Initial DIACAP Package Workflow

The objective of this task is to register the IT system with appropriate C&A entity, prepare a preliminary System Identification Profile (SIP), develop a DIACAP Implementation Plan (DIP), assemble a DIACAP team, and compile all of the artifacts required to obtain an ATO. This package includes system identification information, system mission, functions, and capabilities, system criticality, information sensitivity, and the system concept of operations. This includes a description of the facility where the system resides, the responsible organizations, and individuals assigned to operate the system.

5.1.1.1 Prepare a Preliminary SIP

Program information will be entered into the SIP template to create the preliminary SIP. The most current version of the SIP and all the DIACAP templates can be found in the Xacta IA Manager. The SIP is a living document and will continually be updated throughout the life cycle of the program. The SIP provides the basic description or metadata about the system being certified.

[5] Customers may include users/PMs/System Owners from within or external to the Marine Corps

5.1.1.2 Register IT System with Appropriate C&A Entity

CMP/POR systems and networks must be registered with MARCORSYSCOM C4II IA Division and entered in the Xacta IA Manager database. All other IT systems must be entered in the Xacta IA Manager database by IA personnel prior to the initiation of the C&A process. All systems and networks must be registered in the Department of Defense Information Technology Portfolio Registry, Department of the Navy (DITPR-DON) before any accreditation action can commence.

5.1.1.3 Assemble DIACAP Team

The DIACAP Team will consist of the individuals that are responsible for implementing the DIACAP for the IT System. At a minimum the DIACAP Team must include the MCEN DAA (or his representative), the lead CA representative, IT System PM or SM, the ISSE, the IT System IAM, IAO, and a UR or their representatives.

5.1.1.4 Determining the Type for the Information System

In order to properly implement the MCCAP process, the PM and ISSE must determine the IS type (i.e., AIS application, enclave, outsourced IT-based process, or platform IT interconnection). For guidance on determining the IS type, refer to section 3.0.

5.1.1.5 Initiate DIACAP Implementation Plan

While the details of the system may not be clear at the outset of system development, the mission needs provide a starting point for the development of descriptive information. From the information obtained, the system's general concept and boundaries can be fairly well understood. In either developing or obtaining the description of the system, knowing what components are *not* part of the system is as important as knowing what components *are* part of the system.

Organizations within and external to the Marine Corps must provide this preliminary information. If unable to acquire the documentation or preliminary information due to time constraints then the Marine Corps representative must resolve the issue with the external organization, develop the documentation, or recommend the system be removed from the MCEN.

For systems from other organizations outside of the Marine Corps, all documentation maintained for the IT system must be listed in the DIACAP Package. The documentation shall include but is not limited to vendor documentation of hardware, firmware, software, functional requirements, system manuals, testing and evaluation reports, standard operating procedures, emergency procedures, contingency plans, user and operator procedures, threat and vulnerability analyses, risk assessments, verification reviews, site inspections, and authorization for processing.

5.1.2 Assign IA Controls and Other Requirements

Identifying and assigning applicable IA controls for an IT system is a critical activity in the MCCAP process. There are four basic steps in assigning the IA controls. They include:

- determining the MAC and CL for the IS;
- identifying the baseline IA controls; and
- augmenting the baseline IA controls.

5.1.2.1 Determining the MAC and CL for the Information System

Baseline security controls selection for an IS is based on the initial characterization of the system and any additional controls selected or created based on the initial risk assessment and level of concern by the PM and System Owner. This task verifies the documentation describing the criticality[6] of the IT system in meeting the Marine Corps' mission responsibilities, the type/sensitivity of the information processed, transmitted, and stored by the system, and the need for protective measures. For further detail in regards to the security controls, see DoDI 8500.2 and the DIACAP Knowledge Service.

Determining the MAC and CL for an IS accomplishes two things: (1) validates that the DIACAP Implementation Plan (DIP) describes the proper security controls for the IT system, and (2) helps to identify any additional security controls not contained in the system security documentation.

5.1.2.1.1 Mission Assurance Category (MAC)

Three MAC levels are used to identify the types of controls that will be placed on the IT system. They include:

- MAC III – For systems having a basic level of concern for, integrity and availability. In the DoD this is defined as systems handling information that is necessary for the conduct of day-to-day business, but does not materially affect support to deployed or contingency forces in the short-term. The

[6] System criticality is a measure of the importance of the IT system (including the information it processes, stores, and transmits) and the length of time the system is out of operation before its loss or compromise results in an adverse impact on agency operations, (e.g., loss of life from system failure, inability to meet contingencies, loss of credibility, or damage to the national security). Relate information processed, transmitted, and stored to the three basic protection categories (confidentiality, integrity, availability). For each category, indicate if the level of concern is low, moderate, or high. DoD, DON, and USMC policies, directives, regulations, and/or instructions are consulted for specific guidelines on data classification and special handling requirements. Include a statement of the estimated risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information in the system. System criticality and information sensitivity will affect the level of risk that is acceptable.

consequences of loss of integrity or availability can be tolerated or overcome without significant impacts on mission effectiveness or operational readiness. The consequences could include the delay or degradation of services or commodities enabling routine activities. MAC III systems require protective measures, techniques, or procedures generally commensurate with commercial best practices. All Marine Corps systems, except for public systems, must meet at least this level of evaluation.

- MAC II – For systems having a moderate level of concern for integrity and availability. In the DoD this is defined as systems handling information that is important to the support of deployed and contingency forces. The consequences of loss of integrity or availability are difficult to deal with and can only be tolerated for a short time. The consequences could include delay or degradation in providing important support services or commodities that may seriously impact mission effectiveness or operational readiness. MAC II systems require additional safeguards beyond best practices to ensure assurance. A short moniker would be that loss of a MAC II system would "kill a mission".
- MAC I – For systems having a high level of concern for integrity and availability. In the DoD this is defined as systems handling information that is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness. The consequences of loss of integrity or availability are unacceptable and could include the immediate and sustained loss of mission effectiveness. MAC I systems require the most stringent protection measures. A short moniker would be that loss of a MAC I system would "kill a Marine".

5.1.2.1.2 Confidentiality Level (CL)

Three CLs are used to establish acceptable access factors for DoD IT systems. They Include:

- Public – For systems having a basic level of concern for confidentiality. This classification is reserved for ISs that process Public Information such as public facing websites. Public Information is categorized as Marine Corps information that has been reviewed and approved for public release by the information owner.
- Sensitive – For systems having a moderate level of concern for confidentiality. This classification is reserved for ISs that process Sensitive Information. Sensitive Information is defined as information in which the loss, misuse, or unauthorized access to or modification, could adversely affect national security.

- Classified – For systems having a high level of concern for confidentiality. This classification is reserved for ISs that process Classified Information. Classified Information is defined as information that requires maximum protection against unauthorized disclosure due to concerns for national security.

5.1.2.2 Identifying the Baseline IA Controls

The security controls selection is based on the initial characterization of the system from the DIP and any additional controls selected or created based on the initial risk assessment and level of concern by the PM or System Owner. This task verifies the documentation describing the criticality[7] of the IT system in meeting the Marine Corps' mission responsibilities, the type/sensitivity of the information processed, transmitted, and stored by the system, and the need for protective measures. For further details regarding identifying baseline security controls, see DoDI 8500.2 and the DIACAP Knowledge Service website.

5.1.2.3 Augmenting the Baseline IA Controls

Baseline IA control sets can be augmented with additional IA controls to address special security needs or unique requirements of the IS(s) to which they apply. Augmenting IA controls must neither contradict nor negate DoD baseline IA controls, must not degrade interoperability across the DoD Enterprise, and may not be used as a basis for denying connectivity of systems that have met the DoDI 8500.2 baseline IA controls for MAC and CLs of the system.

5.1.3 Complete and Submit DIACAP Implementation Plan (DIP)

The Department of Defense Instruction (DoDI) 8500.2, IA Implementation and the DIACAP Knowledge Service are resources that are used to answer specific questions about the management, operational, and technical controls of the IT system in order to complete the DIP. In addition to security controls, the DIP also includes the implementation status, responsible entities, resources and the estimated completion date for each assigned IA Control. The DIP also references applicable supporting implementation material and artifacts.

---

[7] System criticality is a measure of the importance of the IT system (including the information it processes, stores, and transmits) and the length of time the system is out of operation before its loss or compromise results in an adverse impact on agency operations, (e.g., loss of life from system failure, inability to meet contingencies, loss of credibility, or damage to the national security). Relate information processed, transmitted, and stored to the three basic protection categories (confidentiality, integrity, availability). For each category, indicate if the level of concern is low, moderate, or high. DoD, DON, and USMC policies, directives, regulations, and/or instructions are consulted for specific guidelines on data classification and special handling requirements. Include a statement of the estimated risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information in the system. System criticality and information sensitivity will affect the level of risk that is acceptable.

5.1.4 DIACAP Implementation Concurrence

Once the DIP is complete, it is submitted to the UR and PM for formal review.

The information in the initial DIP and POA&M can be used to update the SIP. See section 6.0 for the internal documentation process. A certification requirements review (CRR) is held for the certification and accreditation participants and includes the information documented in the DIACAP package, (i.e., mission and system information, operational and security functionality, operational environment, security policy, system security requirements) and the information provided in the POA&M (known security problems or deficiencies, and timelines for mitigation approaches).

For CMP/POR systems and networks in the acquisition process, MARCORSYSCOM will assign a representative from the IA division that conduct a CRR. The CRR is conducted in coordination with the MCEN DAA representative and a MCEN C&A team representative. At this time, the review timeline are established and the required information is entered into the DITPR-DON database.

For ISs and networks originating outside MARCORSYSCOM, the DIP is reviewed and approved by the System Owner, Certifying Authority representative, MCEN Certifier, and MCEN DAA.

5.2 IMPLEMENT AND VALIDATE ASSIGNED IA CONTROLS

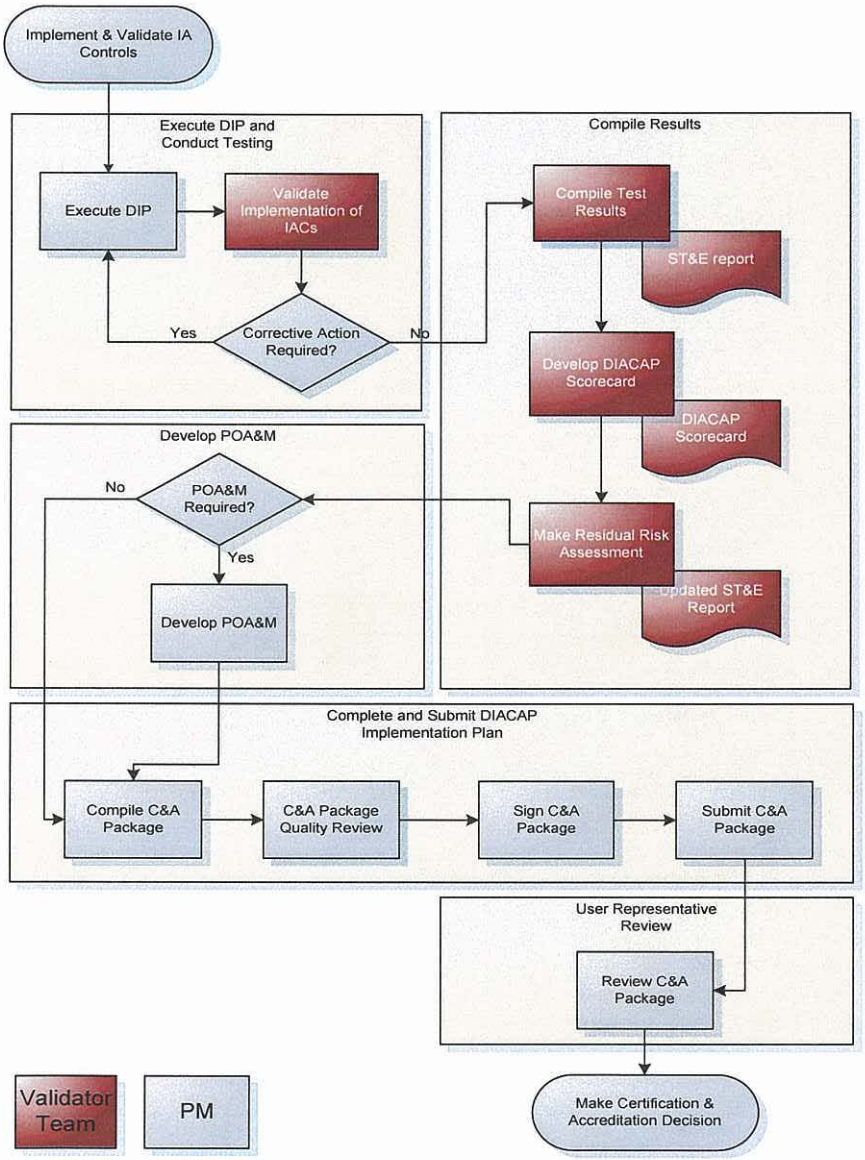


Figure 8 - Implement and Validate IA Controls

To finalize the Implement and Validate Assigned IA Controls phase, one must conduct the following five distinct tasks. They include:

- Execute DIP and Conduct Testing
- Compile Results
- Develop POA&M
- Complete and Submit Final DIACAP Implementation Plan
- User Representative Review

5.2.1 Execute DIP and Conduct Testing

The purpose of this step is to demonstrate through independent assessments using selected verification techniques and verification procedures that the security controls for the IT system have been implemented correctly and are effective in their application. Correct and effective implementation of security controls is a necessary condition to demonstrate compliance with the system security requirements. The results of this phase are documented in the developmental and/or operational validation reports, which are included in the final certification package along with the DIP and final risk assessment report.

These steps are appropriate for new systems, major and minor system upgrades, and legacy systems. Each verification procedure may have a developmental validation component and an operational validation component. Typically, the difference in the developmental and operational verification procedures is in the amount of information available at that particular stage in the system development life cycle.

If a validation has been conducted and submitted as part of a C&A request, the results will be reviewed for accuracy and completeness. The POA&M identifying any security vulnerabilities and planned mitigations is required and will be reviewed for completeness. This effort will also validate Marine Corps operating force and subordinate command Certifier certification statements.

For developmental validations, there are numerous assumptions made about the environment where the system will operate which cannot be fully verified until the system is deployed for operation. The following sections contain descriptions of the certification tasks.

5.2.1.1 CMP/POR Systems

For CMP/PORs, MARCORSYSCOM IA personnel will oversee validation of the IA controls documented in the DIP and evaluate the systems vulnerabilities against threats to identify the risk associated with the planned operation of the system as outlined in

the acquisition and development requirements. For systems and networks going through the acquisition process, MARCORSYSCOM IA personnel will validate IA controls provided by the PMs and evaluate the systems vulnerabilities against threats to identify the risk associated with the operation of the system as designed, and generate a DIACAP Scorecard. MARCORSYSCOM will coordinate any network ports, protocol, or service security issues with the MCEN C&A team to assure an enterprise review is accomplished.

5.2.1.2 Non-CMP/POR Systems

For non-CMP/PORs, the MCEN C&A team or other CA approved entity will validate IA controls documented in the DIP and evaluate the systems vulnerabilities against threats to identify the risk associated with the operation of the system from an enterprise networks and network connections perspective. The IA controls that are not implemented nor have security issues will be noted in the POA&M, and listed with a mitigation strategy.

5.2.1.3 Security Controls Validation Planning

Test plans and procedures include a combination of system developer and system integrator testing as well as additional testing conducted by the validation team during the security certification process. The totality of all testing and evaluation activities addresses all of the security requirements and provides sufficient evidence of the amount of residual risk.

The system security test plan should be developed during the system life cycle program definition and risk reduction phase. This plan flows from the mission, environment, security requirements, and architecture as documented for the system; the results of this testing directly affect decisions made about system certification and accreditation. The system security test plan defines the testing approach, objectives, and procedures for a system. The document can also serve as a program management tool for scheduling activities and resources and as a technical specification for the execution of security testing

5.2.2 Conducting and Analyzing the Security Controls Validation

The objective of this task is to evaluate the technical implementation of the security design and to determine if the security hardware, software, and firmware features affecting confidentiality, integrity, and availability have been implemented as documented in the DIACAP package and that the features perform properly.[8]

---

[8] When a system is developed for deployment to multiple locations a type accreditation may be desirable. In this situation, a Security Controls Validation should occur at a central integration and test facility or at one of the intended operating sites, if such a facility if not available. Software and hardware security tests of common system components at multiple sites are not

This task is: (1) to demonstrate through appropriate verification techniques, verification procedures, and procedure refinements (as needed), that the management, operational, and technical security controls for the IT system are implemented correctly and are effective in their application, and (2) to prepare the final a validation report(s) based on the results of the validation activities carried out during the certification phase.

The security validation verifies the correct implementation of the security functional requirements, (e.g., identification and authentication, access controls, audit) and any other technical security requirements addressed in the DIACAP Package, (e.g., network connection rule compliance). Individual tests evaluate system conformance with the overall requirements, mission environment, and architecture and validate the proper integration and operation of all security features. Some of the validation tests would include:

- Examining the test results and associated test documentation provided by system developer to verify that the system security functions (security features) have been appropriately tested against the functional specification.
- Examining the test results and associated test documentation provided by system developer to verify that appropriate test coverage has been achieved during the testing of the system security functions against the functional specification.
- Testing a subset of the system security functions as appropriate to independently verify that the security functions perform as specified and that the IT system operates as expected.
- Verifying that the IT system satisfies the security requirements for identification and authentication, logical access, and audit, as defined in the DIACAP Package; including the standard security control objectives for confidentiality, integrity, and availability as outlined in DoDI 8500.2 and the DIACAP Knowledge Service.

Documentation of successful security review of applications will be accomplished through the Application Security Plan (ASP).[9]

5.2.3 Compile Results

The validation reporting affects both the certification and accreditation processes, and is included in the DIACAP package.

---

recommended. At the conclusion of the type accreditation Security Controls Validation, the test results, Validator's recommendation, and the type accreditation are documented in the DIACAP Package. This becomes the baseline security requirements at each site where the system will be installed. The site will not need to repeat the baseline test conducted by the type accreditation effort. However, the local system installation and security configuration should be tested at each operational site in the site validation.

[9] See section 3.6.2

5.2.3.1 CMP/POR Systems

For CMP/PORs, the DDAA makes a decision to grant an IATT based on the information provided in the validation report. Once system testing is completed, the conclusions and recommendations are compiled into a validation report and are forwarded to the MCEN DAA for an accreditation decision.

5.2.3.2 Non-CMP/POR Systems

For non-CMP/PORs, the Certifying Authority representative makes a certification decision based on the information contained in the validation report. The MCEN DAA makes an accreditation decision based on the conclusions and recommendations contained in the validation report.

The security test reporting process includes the following:

5.2.3.3 Findings or Discrepancies

When certification activities are performed, the security test team will identify findings or discrepancies that will be divided by level of possible effect on the system or site security baseline. There are four categories for identified findings or discrepancies:

- **Category I**. A significant security finding that must be fixed before a system or site can become operational or must be corrected before an operational system or site can continue to operate. In the DoD this is assigned to findings that allow primary security protections to be bypassed, allowing immediate access by unauthorized personnel or unauthorized assumption of super-user privileges. No accreditations, either interim or full, will be granted with any unmitigated Category I finding.
- **Category II**. A security-related finding that must be fixed within a specific time period for approval (either Interim Authorization to Operate or an accreditation decision) to be granted. In the DoD this is assigned to findings that have a potential to lead to unauthorized system access or activity. Category II findings can usually be mitigated and will not prevent an interim from being granted, but must be fully mitigated before a full accreditation is granted.
- **Category III**. A security-relevant recommendation for which implementation is a program or site option.
- **Category IV**. A non-security-relevant recommendation for which implementation is a program or site option.

Placement of a security finding into one of the four categories requires careful consideration and depends on the following factors:

- The security deficiency
- The relationship of the deficiency to the overall security design
- The role of the component in the system or site baseline infrastructure
- The effect of the deficiency on the system or site security baseline
- The operational environment
- The risk factor.

Resolution of the findings is required so the system or site baseline can be properly maintained. The following methods will be used to ensure correction of any finding:

- A list of all findings will be included in the appropriate test report and provided to the appropriate organization (e.g., PM, IAM, Certifying Authority representative).
- The security test team will provide a POC who is responsible for the resolution of each finding and will define a period of time to allow for correction of the deficiency.
- The appropriate organization (e.g., PM, IAM) will ensure that all findings are corrected within the prescribed time frame.
- At a minimum, the appropriate organization will provide a quarterly status report of all findings to the system's Certifying Authority representative.

The system Certifying Authority may require additional actions for an organization or site to perform as a result of an evaluation of final test results, analyses, or reviews.

5.2.3.4 Test Report

The test report describes the results of the particular tests conducted. It also contains technical evidence that the system has implemented the appropriate safeguards that allow the system to process sensitive or classified data with an acceptable level of risk. Finally, the test report supports the Certifying Authority representative's recommendation for the MCEN DAA to make an accreditation decision.

The security test team will either prepare or review the test report. At a minimum, the test report must include:

- A complete description of the test configuration
- A summary of the test results
- All findings categorized
- Any action items assigned
- Conclusions
- Recommendations

- A Description of completed test procedures

The test report will be forwarded to the appropriate Certifying Authority representative for action on final review by the certification team and added to the IT system's project file in the Xacta IA Management database.

5.2.3.5 Perform a Security Control Objective Review; create the DIACAP Scorecard

The Department of Defense Instruction (DoDI) 8500.2, IA Implementation and the DIACAP Knowledge Service are resources to answer specific questions about the management, operational, and technical controls of the IT system in order to populate the DIACAP Scorecard. The DIACAP Scorecard provides a summary report of all planned for and presently implemented security controls, and the status of the in the IA controls in a format that can be exchanged electronically.

5.2.4 Develop POA&M

If a security validation has been conducted and submitted as part of a C&A request, the results will be reviewed for accuracy and completeness. Any residual vulnerability in the IT system must be entered into a Plan of Action and Milestone (POA&M) document by the PM or system owner. The POA&M then becomes a permanent record of the status of all corrective actions directed in association with an accreditation decision. All security vulnerabilities found in the system and planned mitigations must be documented in the POA&M and reviewed for completeness. This effort also validates Marine Corps operating forces and subordinate command Certifier certification statements. The project entry in the Xacta IA Manager database for the IT system must be updated with the latest POA&M. In order to facilitate the process, all POA&Ms must be entered using **unaltered** copy of the POA&M template located in Xacta IA Manager. POA&Ms that contain classified information will not be entered into the Xacta IA Manager system.

5.2.5 Complete and Submit Final DIACAP Scorecard

This task is to prepare the final certification findings and to assemble the final Accreditation Package for the MCEN DAA. The Accreditation Package, prepared by the appropriate Certifier, includes an updated DIP, developmental and/or operational validation reports, final risk assessment report, and certifier's statement.

The certification findings represent the collective judgment of the certifier and the certification team in assessing the technical correctness and operational effectiveness of the security controls deemed necessary for the IT system. This independent technical and non-technical assessment is intended to provide the MCEN DAA with the most complete information possible regarding the state of the management, operational, and technical controls for the IT system.

The certification findings also recommend to the MCEN DAA the possible implementation of additional risk mitigation actions that would mitigate the residual risks identified as a result of the validation.

Completed system security documentation submitted by Marine Corps operating force or subordinate command's CA representatives for an accreditation decision of **operational** systems need only have a certification endorsement from the MCEN C&A to support a recommendation for accreditation. If systems documentation submitted by Marine Corps operating force or subordinate command's CA representatives fails to receive an endorsement from the MCEN C&A, if a coordinated agreement cannot be reached, sufficient rationale must be documented within the certification package in order to support a MCEN DAA risk-based decision.

Once the MCEN C&A team and the MARCORSYSCOM IA division complete their security assessments, the appropriate Certifier will formally certify the system to the MCEN DAA for the final Accreditation decision. To certify an application, the appropriate Certifier will provide a signed ASP to the MCEN DAA for final approval.

Upon reaching Milestone C, systems in the **acquisition and development** cycle the SYSCOM Certifier will evaluate the system and the DIACAP package will be forwarded to the MCEN C&A team for assessment and validation from an enterprise impact perspective. Once the enterprise assessment is performed, the MCEN C&A forwards the package to the MCEN Certifier for certification and an accreditation recommendation. The MCEN Certifier will forward the completed package to the MCEN DAA for the final Accreditation decision and eventual inclusion into the appropriate enclave DIACAP Package. For systems failing to receive an accreditation endorsement, sufficient rationale must be documented and provided to the MCEN DAA for a risk-based decision.

For operational systems, the specific MEF/MSC/MCI Certifying Authority representative will review the DIACAP package to assist in making their certification determination. The MEF/MSC/MCI CA representative will then submit the DIACAP package to the MCEN C&A team for review.

5.2.5.1 User Representative Review

Once the validation is complete, and the DIACAP Package is updated, the UR is given the opportunity to review the results of the validation and either correct any deficiencies or provide a mitigation strategy to compensate for the vulnerability. Once this process is completed, the DIACAP Package is forwarded to the DAA for accreditation.

5.3 MAKE CERTIFICATION DETERMINATION AND ACCREDITATION DECISION

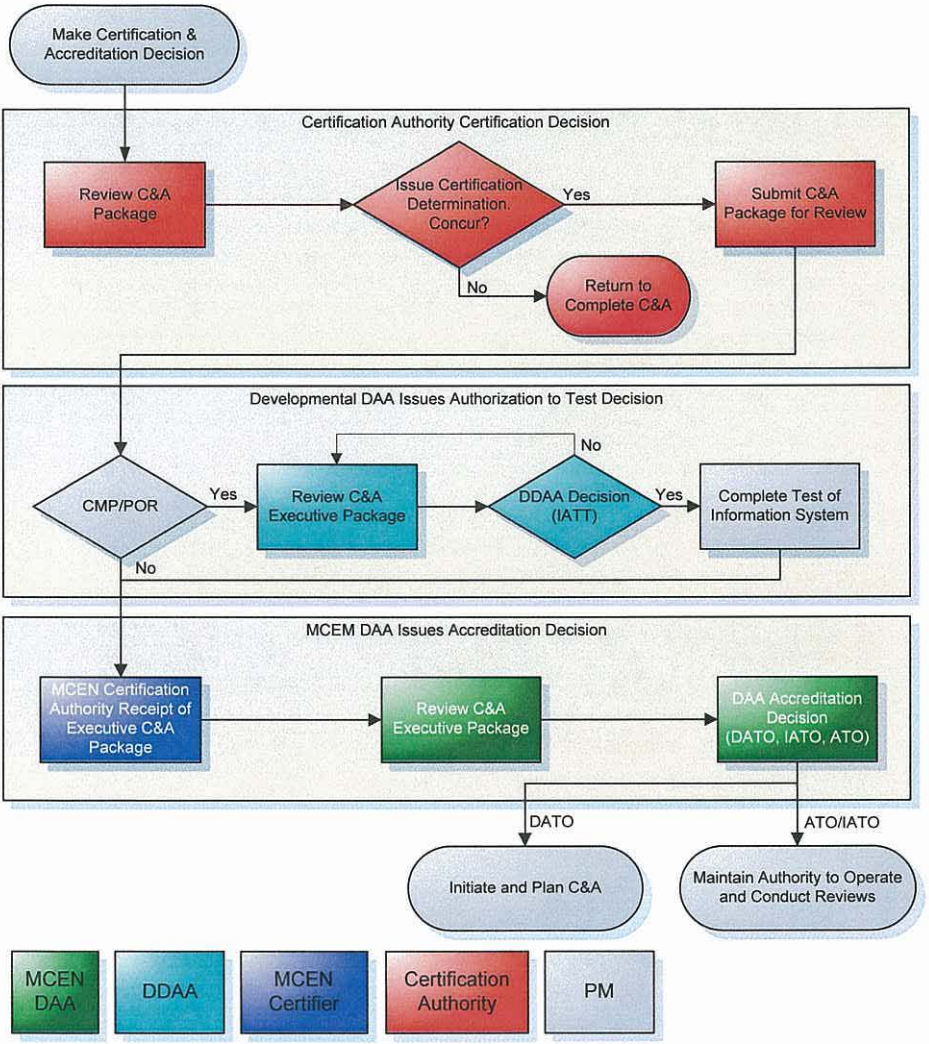


Figure 9 - Make Certification and Accreditation Decision

The purpose of the accreditation phase is to complete the final risk assessment on the IT system, update the DIP, prepare the certification findings, issue the accreditation

decision, and update the Xacta IA Manager database. The final risk assessment takes into account the validation results from the certification phase in determining the residual risk for the system after a thorough and impartial assessment of the correctness and effectiveness of the security controls.

The certification findings bring together all of the relevant information supporting the certification process including the updated DIP, the validation report(s), the final risk assessment report, the certifier's statement into the final Accreditation Package, and update the Xacta IA Manager database. The Accreditation Package contains the principal evidence that the MCEN DAA uses to make an informed, risk-based decision on whether to fully accredit, partially accredit, or not accredit the IT system for operation.

The accreditation phase consists of two tasks:

- Evaluate the Certification Findings; and
- DAA Accreditation Decision.

Upon completion of the accreditation phase, the C&A process moves into its final phase, the post-accreditation phase, which often ends in the demobilization and destruction of a system. The following sections contain descriptions of the accreditation tasks:

5.3.1 Evaluate the Certification Findings

This task determines the residual risk to the IT system based on the results of the validation activities conducted during the certification phase. The residual risk, which is documented in the final risk assessment report, describes the risk remaining for the system after appropriate risk mitigation has occurred, (i.e., security controls implemented, assessed, and corrective actions initiated). The degree of acceptable residual risk is determined by the MCEN DAA (with inputs from the PM or system/data owner) in accordance with the Marine Corps' mission requirements.

The risk assessment examines the system vulnerabilities with respect to the documented threat, ease of exploitation, potential rewards, and probability of occurrence. The operational procedures and safeguards are evaluated to determine their effectiveness and ability to offset risk. The risk assessment quantifies the risks to the IT system and its surrounding environment in the following areas: physical, personnel, administrative, and operating procedures, communications, emanations, hardware, software, and INFOSEC.

A risk is derived from the analysis of a threat-sources ability to exercise vulnerabilities found within the IT system. The purpose of this analysis is to determine if countermeasures are adequate to limit the probability of loss or if the impact of loss is

reduced to an acceptable level. For each residual risk, a statement is made to indicate the rationale for accepting or rejecting the risk and possible future modifications to mitigate the risk. If future solutions are proposed, a tentative implementation schedule is included. The risk assessment is the final review of the system before developing the recommendation to the MCEN DAA. The MCEN DAA determines the acceptable level of risk to protect the system commensurate with its value to the respective organization.[10]

5.3.2 DAA Accreditation Decision

This task is for the MCEN DAA to review the evidence brought forward in the certification package, (i.e., DIP, validation report(s), final risk assessment report, and certifier's statement), and to issue the final accreditation decision for the IT system. This evidence represents the best independent assessment of the correctness and effectiveness of the management, operational, and technical security controls employed to protect the IT system in its operational environment.

The accreditation decision takes into account the state of the security controls for the system and the mission requirements of the agency. After employing the necessary security controls, assessing the correctness and effectiveness of those controls, mitigating any unacceptable risks, the level of risk remaining (residual risk) for the system in performing its operational mission must be within tolerable limits as established by the MCEN DAA.

After receipt of the CA representative's recommendation, e.g. SYSCOM Certifier (for PORs) or the MCEN Certifier, the MCEN DAA reviews the Accreditation Package and makes an accreditation determination. This determination is added to the package. The final Accreditation Package includes the Certifier's formal recommendation, the MCEN DAA accreditation decision, and supporting documentation.

The Accreditation Package must contain all the information necessary to support the CA representative's recommendation including security findings, deficiencies, risks to operate, and actions to resolve any deficiencies. It is with this documented information that the MCEN DAA considers the remaining risk to the system and decides whether or not to authorize processing, placing the system into operation and accepting the residual risk.

The MCEN DAA has the responsibility of accrediting an IT system before it is allowed to connect to the network. Based on the given situation, the MCEN DAA will choose

---

[10] An acceptable level of residual risk is based on the relationship of the threat to the system and the information processed; to the system's mission, environment, and architecture; and to the system's security objectives.

one of the following accreditation options when rendering a final accreditation decision: (1) *full accreditation*, (2) *interim accreditation*, or (3) *accreditation disapproval*.

5.3.2.1 Full Accreditation

If the CA representative concludes that the integrated system satisfies the system security technical requirements, they issue a system certification. The systems certification certifies that the system has complied with the documented security requirements. Supplemental recommendations might also be made to improve the system's security posture. Such recommendations should provide input to future system enhancements and configuration management decisions.

In the case of full accreditation, the system security requirements have been satisfied and the security controls have been implemented correctly and are operating effectively. The system is approved to operate in the intended environment as stated in the DIP and few, if any, restrictions on processing apply. The MCEN DAA issues an appropriate accreditation letter along with any supporting documentation justifying the accreditation decision.

System accreditation decisions by the MCEN DAA are conveyed in the DAA letter. When combined with the certification results and associated letters, this becomes the final Accreditation Package. In most cases, the basis for accreditation can be constructed from information provided in the certification documentation. Certain information from the DIP, validation reports, and risk assessment report may, at the discretion of the MCEN DAA, be withheld in the final Accreditation Package due to its sensitive nature.

In some situations a common set of software, hardware, and firmware is installed at multiple locations. Since it is difficult to accredit the common systems at all possible locations, the MCEN DAA may issue a type accreditation for a typical operating environment.

The type accreditation is the official authorization to employ identical copies of a system in a specified environment. [11] The accreditation package must be modified to include a statement of residual risk and clearly define the intended operating environment. The appropriate documentation must identify specific uses of the system, operational constraints and procedures under which the system may operate. In that case, the DAA would include a statement with the accreditation, such as:

> "This system is supplied with a type accreditation. With the type accreditation, the operators assume the responsibility to monitor the environment for

[11] See section 3.6

compliance with the environment as described in the accreditation documentation."

The PM, UR, and IAM/IAO should ensure the proper security operating procedures, configuration guidance, and training is delivered with the system.

5.3.2.2 Interim Accreditations

In some cases, the CA representative may uncover security deficiencies, but continue to believe that the short-term system operation is within the bounds of acceptable risk. They may recommend an interim accreditation with the understanding that deficiencies will be corrected in a time period specified by the MCEN DAA. These deficiencies must be reflected in the security documentation and an agreement obtained on the conditions under which the system may be operated and the date by when the deficiencies will be remedied. These are noted as Interim Authorizations to Operate (IATO)

An interim accreditation may also apply to temporary connections to a network backbone or router for access to network assets. These are noted as Interim Authorizations to Connect (IATC). In the acquisition and development process, the Developmental DAA issues Interim Authorizations to Test (IATT) to allow PMs to evaluate systems and components on a test network or environment, to assure appropriate design and implementation.

For interim accreditations, the system does not currently meet the security requirements as stated in the DIP and all of the necessary security controls are not implemented and operating effectively. However, mission criticality mandates the system become operational and no other capability exists to adequately perform the mission. The interim accreditation is a temporary approval that may be issued for a limited period of time as specified by the MCEN DAA.

Pending accreditation, an interim accreditation is normally permitted, provided the following conditions are satisfied:

- The tasks identified in the Initial Assessment activity are completed[12].
- The security POA&M, which has the identified risks and mitigations, has been completed and signed
- A DIP has been developed to prevent unauthorized disclosure of data. The normal operational procedures for the users may have to be altered (i.e., limited) until full accreditation is achieved.
- A schedule describing the advancement to the final accreditation must be established. Dates may be used, if this is applicable; however, the schedule will frequently be event-driven (e.g., completion of software tests or

[12] See section 5.1

operational security analysis). The schedule must be mutually satisfactory to the system owner and the MCEN DAA.

Three typical cases where Interim Authorization to Operate (IATO) will be employed are:

- A new IT system is in an advanced test phase and must use some actual operational data for final design and test before initial operational capability. The SYSCOM Certifier will provide the certification recommendation for these cases.
- An initial risk assessment has concluded that there are no apparent security problems that would allow unauthorized persons to access data in the IT system, but there has not been sufficient time or resources for rigorous hardware and software testing to determine, for example, whether need-to-know restrictions are fully implemented.
- The configuration of an operational IT system has been altered. Initial security evaluation by appropriate personnel does not reveal any severe problems, but a full evaluation has not been completed.

An IATO can be requested after any assessment action, but certain activities must be completed.

If the MCEN DAA is inclined to issue an IATO, the operational restrictions imposed to mitigate the increased risk should be carefully reviewed, and an interim accreditation action plan should be developed that acknowledges the following:

- Mission criticality necessitates immediate operation of the system;
- Interim accreditation approval is in the best interest of the organization;
- Resources are available to complete the action plan and the needed certification tasks;
- The action plan can be completed within the allowable time specified by the MCEN DAA; and
- Operational restrictions lessen the risk to the lowest level possible (at this time) and the residual risk is acceptable.

The MCEN DAA issues an appropriate interim accreditation letter conveying the above conditions and restrictions and providing supporting documentation, as necessary.

5.3.2.3 Accreditation Disapproval

If the CA representative determines that the system does not satisfy the security requirements and that short-term risks place the system operation or information in jeopardy, they must recommend that the system not be accredited.

In the case of accreditation disapproval, the system does not meet the security requirements and security controls as stated in the DIP, residual risk is too great, and mission criticality does not mandate the immediate operational need. Therefore, the developmental system is not approved for operation or, if the system is already operational, the operation of the system is halted. The MCEN DAA issues the appropriate accreditation disapproval letter including any supporting documentation justifying the accreditation disapproval decision.

In the Marine Corps some cases of mission need may drive the MCEN DAA to grant a limited accreditation to connect and operate, even though a CA representative may recommend disapproval. Before this particular decision is reached, the MCEN DAA must coordinate in advance with the CA representative in question, the SYSCOM Certifier if it affects a CMP/POR system, the MCEN Certifier, and the MCEN Validator to determine the most appropriate course of action for the good of the Marine Corps. This type of decision will have specific boundaries, implementations, participants, and time-lines that must be met.

5.4 MAINTAIN AUTHORITY TO OPERATE AND CONDUCT REVIEW

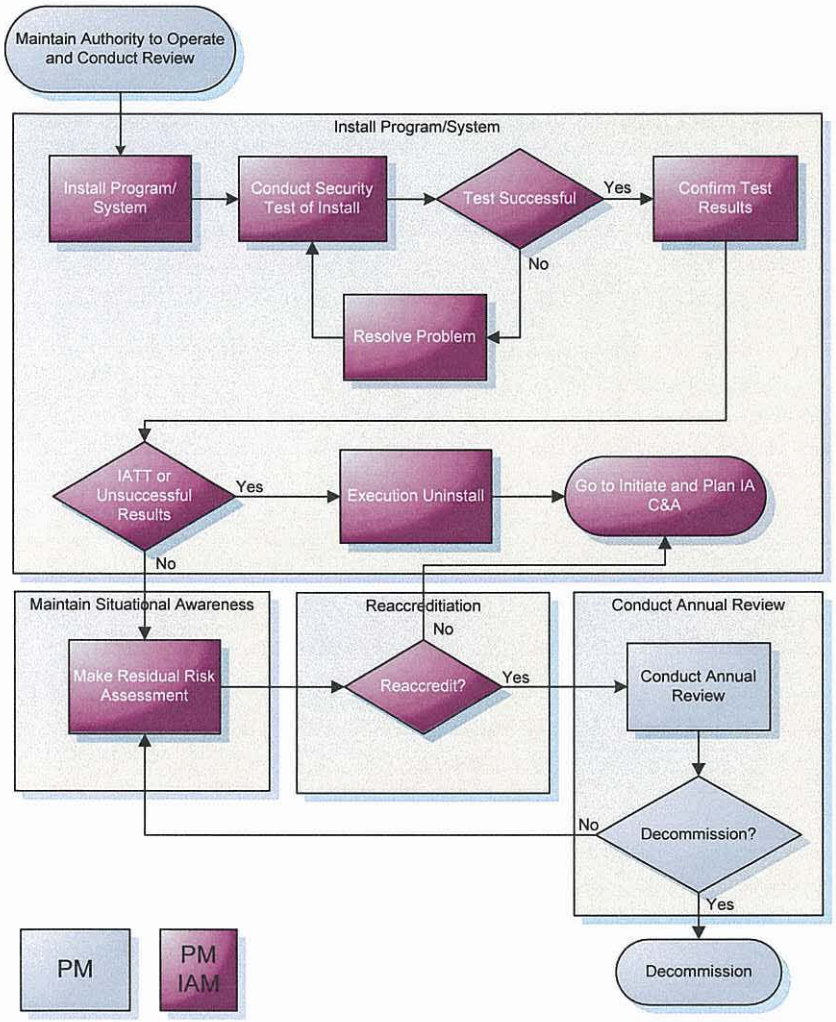


Figure 10 - Maintain Authority to Operate and Conduct Review

The IAM/Program owner is responsible to provide an annual assessment to the MCEN DAA, and the MCEN Certifier, based on the review of all IA controls and testing of selected IA controls as required by FISMA that either confirms the effectiveness of

assigned IA controls and their implementation or recommends changes. PMs of CMP/POR systems and networks must also include the MARCORSYSCOM IA Division in those assessment reports.

The monitoring activity is necessary to ensure an acceptable level of residual risk is preserved for the system. When changes to the system or to the system's operational/threat environment are deemed significant to the security of the IT system, reaccreditation activities are initiated.

The Maintain Authority to Operate and Conduct Review phase consists of four tasks that provide for continual IT Security Assurance. They are:

- Install Program/System;
- Maintain Situational Awareness;
- Reaccreditation; and
- Conduct Annual Review.

The post-accreditation phase is a continuous process that is necessary to address the dynamic nature of agency missions and the rapidly changing technologies employed by agencies to support those missions. The following sections contain descriptions of all post-accreditation tasks and associated subtasks.

5.4.1 Install Program/System

Once an IT system has been granted an Authorization to Operate (ATO) or an Interim Authorization to Operate (IATO) from the MCEN DAA, it can then be placed into the production environment.

5.4.2 Maintain Situational Awareness

The objective of this task is to carefully track all modifications to the IT system or its supporting operational environment. The MCEN DAA, PM, and system owner must be vigilant in maintaining the security posture of the system.

Changes to the system may affect the way security controls work or may create new vulnerabilities. Likewise, the environment provides a certain amount of security protection to the system and must be continuously monitored for changes that might affect the security posture of the system.

Strong configuration management practices ensure that all system modifications are documented—the first step in assessing the potential impact of those changes to the security of the system.

Continuous improvements to the system must be able to occur without necessarily triggering the reaccreditation process. To accomplish this type of controlled change, each modification, proposed or actual, is assessed for its potential impact on the security of the system.

After the system modification is completed and it is verified that the change does not affect the security of the system, the DIACAP Package is appropriately updated. If the security of the system is affected, a reaccreditation may also be initiated.

5.4.3 Reaccreditation

The objective of this task is to identify significant changes to the IT system or its surrounding operational environment that necessitate reaccreditation. The MCEN DAA, in consultation with the PM or system owner, determines the conditions under which the system must be reaccredited. Reaccreditation can be either event-driven or time-driven depending on the laws, regulations, directives, instructions, or policies which dictate such activity.

OMB Circular A-130 requires reaccreditation every three years or whenever significant changes occur to a system. DoD requires annual security reviews. The reaccreditation of the system begins with the pre-certification phase and consists of all tasks completed during the original C&A process. Depending on the nature and extent of the modifications to the system and its supporting environment, a significant portion of the original certification documentation and validation results may still be applicable. Reuse of previous certification evidence is an effective method of reducing assessment costs during the reaccreditation process.

5.4.4 Conduct Annual Review

The objective of this task is to ensure that a comprehensive annual IA review is performed to evaluate existing policies and that procedures are consistent to support uninterrupted operations. FISMA requires revalidation of a select number of IA controls at least annually. The development of any newly identified threats and vulnerabilities also may necessitate a review of: (1) the levels of concern for confidentiality, integrity, availability, and system exposure, (2) the security controls, and (3) the certification level, to ensure the system remains adequately protected. The IAM may, independently or at the direction of the MCEN DAA, schedule a revalidation of any or all IA controls to correct any deficiencies found during the annual review.

5.5 DECOMMISSION

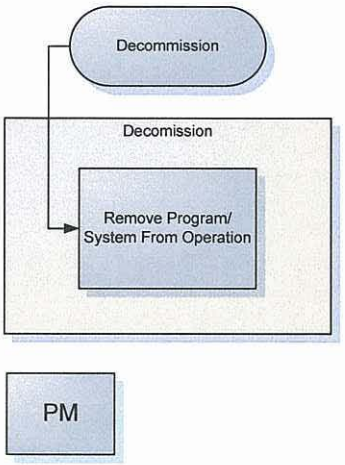


Figure 11 - Decommission Information System

The objective of this task is to ensure that an IT system reaching the end of its life cycle, and having been identified for disposal, is taken out of the operational environment and disposed of in a secure manner. There are three important areas of concern that must be addressed when a system has been identified for elimination: (1) the archival of information, (2) the disposal of hardware, firmware, and software, and (3) the sanitization of media.

6.0 CIRCUIT CONNECTION APPROVAL DOCUMENTATION

Once approved by the Marine Corps Circuit Management Office (MCMO) to acquire a circuit, a unit will complete a DISA Circuit Questionnaire to apply to connect to the GIG backbone. All questionnaires, either NIPRNET Circuit Questionnaires (NCQs) or SIPRNET Questionnaires (SCQs) will be completed by the requesting Marine Corps organization, listing the MCEN DAA contact information as the DAA.

The NCQ/SCQ will be submitted to the MCEN C&A section, which will validate the security statements contained and then forward to the DAA for signature. Once signed, the MCEN C&A section will transmit the documentation to the DISA Connection Approval Office.

All permanent and garrison circuits in the Marine Corps will be accredited by the MCEN DAA. Units will forward their NCQ/SCQ documentation through the MCNOSC for accreditation.

Circuits acquired in support of a Combatant Command for a one-time use, e.g., an exercise, a task-force in response to a catastrophic event, can be approved by the local G-6, but must inform the MCNOSC and MCEN DAA of the circuit and the estimated duration of use.

6.1 IAM/IAO:

- Collects initial IA information and any supporting documentation.
- Compares to applicable C&A requirements in accordance with DoD, DON, and Marine Corps policy.
- Identifies deficiencies and executes the necessary C&A processes to correct, if required
- Documents results and forwards along with a recommendation through the G-6 to the DAA
- Develops the request for MCEN connection and all related documentation to forward through the G-6 to the MCEN C&A team.

6.2 COMMAND G-6 (CA REPRESENTATIVE):

- Verifies the accreditation and support documentation is current and accurate
- Submits the MCEN Connection Request to the MCEN DAA
- Remediate command discrepancies in accordance with MCEN DAA direction

6.3 MCEN DAA AND SUPPORT STAFF:

- MCEN C&A team reviews the Connection Request and forwards recommendation to the DAA
- MCEN DAA makes determination (approval/disapproval) within 10 working days, and provides the decision to the Command G-6, e.g., provides specific details and a way ahead for achieving approval, if disapproved.

7.0 REFERENCES

This appendix provides a list of relevant statutes, regulations, directives, and other guidance applicable to IT security and critical infrastructure protection (CIP). It includes those cited in this document as well as other items that concerned personnel might need to understand. Although it is not a comprehensive collection of IT security-related references and authorities, it is sufficiently detailed to facilitate the reader's use of this document and to understand other IT security-related documentation.

a. COMNAVNETWARCOM ALCOM 093/06, *Establishment of Roles and Responsibilities for DON IT Certification and Accreditation Process*, September 2006

b. Chairman of the Joint Chiefs of Staff Manual (CJCSM) No. 6510.01, *Defense in Depth: Information Assurance (IA) and Computer Network Defense (CND) Manual*, 14 August 2006

c. DoD Chief Information Officer, *Interim Department of Defense (DoD) Information Assurance (IA) Certification and Accreditation (C&A) Process Guidance*, 6 July 2006

d. Committee on National Security Systems Instruction (CNSSI) No. 4009, *National Information Assurance (IA) Glossary*, revised June 2006

e. MARADMIN 018/06, *Establishment of the Marine Corps Information Assurance Division*, 17 January 2006

f. Committee on National Security Systems Policy (CNSSP) No. 6, *National Policy on Certification and Accreditation of National Security Systems*, October 2005

g. SECNAV M-5239.1, *Department of the Navy Information Assurance Program*, November 2005

h. SECNAVINST 5239.3A, *Department of the Navy Information Assurance (IA) Policy*, 20 December 2004

i. DoD Instruction (DODI) 8580.1, *Information Assurance (IA) in the Defense Acquisition System*, 9 July 2004

j. Chairman of the Joint Chiefs of Staff Instruction (CJCSI) No. 6510.01D, *Information Assurance (IA) and Computer Network Defense (CND)*, 15 June 2004

k. CNSSI 4012, *National Training Standard for Senior System Managers*, June 2004

l. National Security Telecommunications and Information Systems Security Directive (NSTISSD) No. 11, *National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products*, June 2003

m. DoD Instruction (DODI) 5000.2, *Operation of the Defense Acquisition System*, 12 May 2003

n. DoD Instruction 8500.2, *Information Assurance (IA) Implementation*, 6 February 2003

o. Marine Corps Order (MCO) 5239.2, *Marine Corps Information Assurance Program (MCIAP)*, 18 November 2002

p. DoD Directive 8500.1, *Information Assurance (IA)*, 24 October 2002

q. DoD Directive 8100.1, *Global Information Grid (GIG) Overarching Policy*, 19 September 2002

r. Marine Corps CIO charter, 9 September 2002

s. DoD 5000.2-R, *Mandatory Procedures for Major Defense Acquisition Programs (MDAPS) and Major Automated Information System (MAIS) Acquisition Programs*, 5 April 2002

t. Section 3541 of title 44, United States Code, *Federal Information Security Management Act of 2000* (FISMA)

u. *U.S. Marine Corps Project Officers Certification and Accreditation Handbook*, version 3.0, September 2000

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

w. NSTISS No. 600, *Communications Security (COMSEC) Monitoring*, 10 April 1990

x. National Security Decision Directive (NSDD) Number 145, *National Policy on Telecommunications and Automated Information Systems Security*, 17 September 1984

y. IA Operation Standards

z. CJCSI 6510.04, *Information Assurance Metrics*

aa. CJCSI 6510.01, *Defense-in-Depth*

Marine Corps Publications

bb. Marine Corps Departmental Manual 375, Chapter 19, Information Technology Security Program, April 15, 2002.

cc. Marine Corps Departmental Manual 441, Personnel Security.

dd. Marine Corps Departmental Manual 444, Physical Security.

ee. Marine Corps Information Technology Security Plan, Version 2, April 15, 2002.

ff. Marine Corps System Security GSS Planning Guide and Template, April 30, 2002.

gg. Marine Corps System Security MA Planning Guide and Template, April 30, 2002.

hh. Marine Corps Risk Assessment Guide, April 30, 2002.

ii. Marine Corps IT System Contingency Planning Guide, April 30, 2002.

jj. Marine Corps Critical Asset Valuation Guideline, April 15, 2002.

Other Publications

kk. Presidential Decision Directive 63, Protecting America's Critical Infrastructures, May 22, 1998.

ll. Federal Sector Critical Infrastructure Planning Guide, 1998.

mm. Vulnerability Assessment Framework, October 1998.

ENCLOSURE A – ACRONYMS

Acronym	Definition
ACTD	Advanced Concept Technology Demonstration
AIS	Automated Information System
ASP	Application Security Plans
ATO	Authorization to Operate
C&A	Certification and Accreditation
C4	Command, Control, Communications and Computers
C/NC	Compliant/Non-compliant
CA	Certifying Authority
CIO	Chief Information Officer
CJCSI	CJCS Instruction
CL	Confidentiality Level
CMP	Centrally Managed Programs
COI	Communities of Interest
CRR	Certification Requirements Review
DAA	Designated Accrediting Authority
DATO	Denial of Authorization to Operate
DCID	Director Central Intelligence Directive
DIACAP	DoD Information Assurance Certification and Accreditation Process
DIP	DIACAP Implementation Plans
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DITPR	Defense Information Technology Portfolio Repository
DMS	Defense Messaging System
DNI	Director of National Intelligence
DoD	Department of Defense
DoDD	DoD Directive
DoDI	DoD Instruction
EAL	Evaluation Assurance Level
EIE	Enterprise Information Environment
FISMA	Federal Information Security Management Act
GIG	Global Information Grid
HQMC	Headquarters Marine Corps
IA	Information Assurance
IAM	Information Assurance Manager
IAO	Information Assurance Officer
IATC	Interim Authorization to Connect
IATO	Interim Authorization to Operate

Acronym	Definition
IATT	Interim Authorization to Test
IC	Intelligence Community
ID	Identification
IS	Information System
ISSE	Information Systems Security Engineer/Engineering
ISSM	Information Systems Security Manager
IT	Information Technology
JCIDS	Joint Capabilities Identification and Development System
KS	Knowledge Service
MA	Mission Area
MAC	Mission Assurance Category
MAIS	Major Automated Information System
MARCORSYSCOM	Marine Corps System Command
MC	Mission Critical
MCCAP	Marine Corps Certification & Accreditation Process
MCEN	Marine Corps Enterprise Network
MCIAP	Marine Corps Information Assurance Program
MCNOSC	Marine Corps Network Operations & Security Center
ME	Mission Essential
MOA	Memorandums of Agreement
MOU	Memorandums of Understanding
MS	Mission Support
MS-A, B or C	[Acquisition] Milestone A, B, or C
NIPRNET	Non-Classified Internet Protocol Router Network
NSA	National Security Agency
NSS	National Security Systems
NSTISSP	National Security Telecommunications and Information Security Policy
OMB	Office of Management and Budget
OSD	Office of the Secretary of Defense
PM or SM	Program or System Manager
POA&M	Plan of Action and Milestones
POC	Point of Contact
POR	Program of Record
PPBE	Planning, Programming, Budgeting and Execution
PPSM	Ports, Protocols and Services Management
SAP	Special Access Program
SAR	Special Access Requirement
SCI	Sensitive Compartmented Information
SDLC	System Development Life Cycle

Acronym	Definition
SEP	System Engineering Plan
SIAO	Senior Information Assurance Officer
SIP	System Identification Profile
SIPRNET	Secret Internet Protocol Router Network
SLC	System Life Cycle
UR	User Representative

ENCLOSURE B - SAMPLE CAR ASSIGNMENT LETTER

Sample Certification Authority Representative Letter

5239

C4/IA
XX XX 08

From: Designated Accrediting Authority (DAA), Headquarters United States Marine Corps (HQMC), Command, Control, Communications and Computers (C4)
To: [INSERT NAME, COMMMAND]

Subj: CERTIFICATION AUTHORITY REPRESENTATIVE (CAR) APPOINTMENT LETTER

Ref: (a) DoDI 8510.01, Department of Defense Information Assurance Certification and
Accreditation Process (DIACAP) of 28 Nov 07
(b) DoDI 8500.2, Department of Defense Information Assurance Implementation of 6
Feb 03
(c) CJCSI 6211.02B, Defense Information System Network (DISN): Policy, Responsibilities and Processes of 31 Jul 03
(d) CJCSM 6510.01, Defense-In-Depth: Information Assurance (IA) and Computer Network Defense (CND) of 25 Mar 03 W CH1
(e) DoDI 8500.2 Information Assurance (IA) Implementation of 6 Feb 03

1. By authority granted in reference (a), you are hereby appointed as a Certifying Authority Representative. You are directed to become familiar with and adhere to all applicable Information Assurance and Information Security directives and policies published by the Department of Defense, National Security Agency, Department of the Navy and the United States Marine Corps.

2. Per reference (c), you have 60 days from the date of this designation to complete the DAA training and certification requirements.

3. As a CAR, you are an official acting on behalf of the CA. Your responsibilities include the following:

- Ensure that the Common Criteria requirements for IA and IA-enabled products are identified and documented prior to contract negotiations.

- Evaluate the system's robustness requirements and mission and customer needs and recommend a specific Evaluation Assurance Level (EAL) for a particular product to the MCEN DAA.
- Test, validate, and document the product's ability to meet the EAL.
- Provide the MCEN DAA with sufficient information to make a risk determination about a non-NIAP-evaluated product.
- Identify and document product security requirements that were unmet or non-compliant.
- Develop and execute component-level tests to assess the risk of unmet security requirements to assist the DAA in determining the information system's overall risk of compromise.
- Verify that all IA and IA-enabled IT products are configured in accordance with DISA and/or NSA Security Technical Implementation Guidelines (STIGs) and Security Recommendation Guides (SRGs) as directed by the MCEN DAA.
- Review all changes to the MCEN for IA impact.
- Ensure that the Contracting Officer incorporates into the contract requirements based on the MAC, security classification, sensitivity, and need-to-know of information and information systems in accordance with reference (b), the permissible uses of information and associated mission or business rules of use, and the distinction between information that is operationally sensitive and information that can be made available to the public.
- Coordinate with the DAA, CA and the PM/SM to ensure that system security requirements are identified, resourced, and implemented to provide an acceptable level of risk.
- Work with the DAA, CA, PM/SM, User Representative, and information owners to ensure that appropriate IA resources are identified and acquired during the initial C&A Phase.
- State any unique requirements for each information system to be accredited in the certification documentation.
- Continuously assess and guide the quality and completeness of C&A activities and tasks and the resulting artifacts.
- Coordinate security requirements with the DAA, the CA, the PM, and the User Representative.
- Coordinate with the User Representative, DAA, PM and CA on determining the Mission Assurance Category (MAC) and Confidentiality Level (CL) of developing systems, in addition to the proper certification levels.

4. You will provide and maintain all CAR requisite training and certification documentation with the local Information Assurance Manager (lAM) and maintain as part of your official personnel file.

5. Questions may be directed to the MCEN DAA at DSN 223-3490 or (703) 693-3490.

RAY A. LETTEER

Copy to:
File
Local Command IAM

ENCLOSURE C - SAMPLE IAM/IAO ASSIGNMENT LETTER

Sample Information Assurance Manager/Information Assurance Officer Assignment Letter

IN REPLY REFER TO:
5500
CAR
DD MMM YY

From: Certifying Authority representative, COMMAND NAME
To: Rank, FName MI LName, USMC

Subj: APPOINTMENT AS COMMAND NAME INFORMATION ASSURANCE MANAGER/OFFICER (IAM/IAO)

Ref: (a) DoDD 8500.1, Information Assurance
(b) DoDI 8500.2, Information Assurance Implementation
(c) MCO 5239.2 Marine Corps Information Assurance Program

1. In accordance with the references, you are hereby appointed as the command Information Assurance Manager/Officer (IAM). You will be guided by the references in the execution of your duties.

2. You will serve as a primary point of contact for all command network and information assurance concerns. You will ensure that an information assurance program is implemented. As a command information assurance POC, you will:

a. Assess the organization's information technology and ensure an adequate information assurance staff is in place to protect the command's information systems. The information systems security staff consists of Information Assurance Manager (IAM), Information Assurance Officers (IAO's), Information Assurance Technicians (0689), Network and System Administrators, and Information Systems Coordinators (ISCs).

b. Provide oversight to the information systems security staff.

c. Ensure that organization information technology is operated within an acceptable level of risk as established by the Marine Corps Enterprise Network (MCEN) Designated Approving Authority (DAA).

d. Ensure that all information systems security related incidents and violations are immediately reported, properly investigated, and correctly resolved.

e. Ensure that all changes to information systems or the system security staff is evaluated from a security viewpoint prior to implementation.

f. Ensure that security plans for information systems are developed and maintained.

g. Confirm the integrity and security of the command network(s) using only those Secure Configuration and Compliance Validation (SSCVI) and Secure Configuration Remediation (SCRI) tools that you have been properly trained and validated in their use.

FI. MI. LNAME

Copy to: Files

FIRST ENDORSMENT on COMMAND INFORMATION ASSURANCE (IA) LTR 5500 DD MMM YY

From: RANK FNAME MI LNAME, USMC
To: Certifying Authority representative, COMMAND NAME

Subj: APPOINTMENT AS COMMAND NAME INFORMATION ASSURANCE MANAGER (IAM)

1. I have read and understand the references and have assumed all duties and responsibilities with my appointment as the COMMAND NAME Information Assurance Manager/Officer.

FI. MI. LNAME

Copy to: Files
MCNOSC

ENCLOSURE D - NIPRNET CIRCUIT QUESTIONNAIRE (NCQ)

NIPRNet Circuit Questionnaire

Date:

DISA Package Number (Assigned by the DISA NCAO): _____
Command Communications Service Designator (CCSD) / Circuit Identifier (e.g., COINS) / or Router Port (RTPS), and/or Satellite Access Request (SAR/GAA Nr.):

COINS
vBNS+:

Organization
Location:
Organizational DMS Address: _____
Enclave/Network ISSM:
Enclave/Network ISSM Email Address:
Enclave/Network ISSM Phone Number:
Technical POC:
Technical POC Email Address:
Technical POC Phone Number:
Administrative POC:
Administrative POC Email Address:
Administrative POC Phone Number:
Fax Number
System or Network Name:
Premise Router IP Address: See Table
Network IP Address Ranges: See Table

Circuit Provider	CCSD/Identifier	Premise Router IP	IP Range	Comments

This form is to be submitted with all initial requests for DOD, Non DOD, Contractor, & Foreign National connections, including exercise and tactical connections. Additionally, this form is to be re-accomplished when there is a change to the approved configuration, certification, and/or a change that affects the answers on file.

Highlight your responses below in yellow.

Combatant Command, Service, or DOD Agency Sponsor/Joint Staff Validation/OSD Approval

(Mandatory for Foreign National, Contractor, and Non-DoD Activities

#1 Yes No Does this connection support a Non-DoD, Contractor, Foreign National user connection or Cross Domain Solution (CDS)?

(Reference CJCSI 6211.02B, Appendix D to Enclosure C – If "YES", the sponsoring agency must submit a requirement letter to Joint Staff, J-6, for validation and OSD approval. A copy of the JS validation and OSD approval must be provided to the NCAO with the NIPRNet Connection Approval Process package.)

#2 Yes No N/A Has the Combatant Command, Service or DoD Agency submitted a sponsorship letter to the Joint Staff (J6T)?

(If yes, a copy of the sponsor's memorandum request must be provided to the NCAO with the NIPRNet Connection Approval Process package.)

#3 Yes No N/A Have the Joint Staff (J6) validated and OSD approved the request for NIPRNet Access/Connectivity?

Non-DoD Facility Access & Connections

#4 Yes No Do uncleared individuals have physical access to Non-DoD facility areas where work centers, terminals, or equipment connect directly or indirectly to the NIPRNet?

(Example: If Non-DoD personnel, either in support of a Non-DoD Government contract or maintenance support, to include cleaning people, have access to areas where NIPRNet workstations are located, a Yes response is required)

Contractor Facility Access & Connections

#5 Yes No Do uncleared contractors **have physical access to areas** where workstations are **connected directly or indirectly** to the NIPRNet?

(Example: If uncleared contractor personnel, either in support of a Government contract or maintenance support, to include cleaning people, have access to areas where NIPRNet workstations are located, a Yes response is required)

#6 Yes No Are cleared contractors at a non-DoD facility **users** on workstations **connected directly or indirectly** to the NIPRNet? Contract Number(s): .

(Example: Any contractor (Prime or Sub) at a non-DoD facility (including Contractor facilities) that connects to the NIPRNet or on a separate network such as an Educational Facility that is logically or physically connected/interfaced to the users network, a Yes response is required.)

#7 Yes No Reference question #6. Are there any uncleared personnel providing support under this contract?

(Example: Any contractor personnel (Prime or Sub) that are providing administrative, logistical or services in

support of the contract identified in number 6, a Yes response is required.)

Foreign National Access

#8 Yes No Do Foreign Nationals, to include Liaison Officers (Foreign nationals in US positions), **have physical access to areas** where workstations **connect directly or indirectly** to the NIPRNet?

(Example: If other than US personnel have access (escorted or unescorted) to the NIPRNet workstation areas, a Yes response is required.)

#9 Yes No Are Foreign Nationals, to include Liaison Officers, **users** on workstations on a network or subnet **connected directly or indirectly** to the NIPRNet?

(Example: If other than US personnel have user accounts on NIPRNet workstations, a Yes response is required.)

Network Connectivity

#10 Yes No Is the activity's NIPRNet network, to include subnet(s) and workstation(s), physically/logically connected or interfaced to a network or platform operating at any level other than Unclassified but Sensitive Only? This includes tunneling, switches, or connections **with or without high assurance guards** in place? Include the Cross Domain Solution (CDS) Ticket Number (if Applicable) :

(Example: A network operating at Unclassified Sensitive, a Yes response is required. This includes configurations where the other network is cryptographically isolated (tunneled).)

If any of the above statements were answered with a **"YES"**, provide a **detailed** description of the systems involved, the security controls employed, information shared, allowed accesses, number of foreign nationals, etc. and identify the Designated Approval Authority for that connection. Please be sure to sign and include the reference number on any and all attachments. Any questions may be directed to DISA, NIPRNet Connection Approval Office (NCAO) at (703) 882-0281, DSN: 381-0281. If the document and its attachments are unclassified after completion you may fax it to COMM (703) 882-2885 or DSN 381-2885.

CERTIFICATION: I certify that the information provided in this document and all attachments are accurate.

_____

Signature Block
Designated Approving Authority (DAA)

ENCLOSURE E - SIPRNET CIRCUIT QUESTIONNAIRE (SCQ)

SIPRNet Circuit Questionnaire (SCQ)

Date: _____

DISA Package Number (Assigned by the DISA SCAO): _____
SIPRNet Command Communications Service Designator(s) (CCSD) / Circuit Identifier (e.g., COINS), and/or Satellite Access Request (SAR/GAA Nr.): _____
Collocated NIPRNet CCSD(s): _____
Organization (Combatant Command/Service/Agency/Sub-Agency/Contractor Name):

_____

_____

Organization Address (DAA Mailing Address):

_____

_____

Point of Presence (POP) Location (Bldg, Room, Base/Pos/Camp/Mobile Platform:

_____

_____

_____

Organizational DMS Address: _____
Enclave/Network DAA and Phone Number: _____
Enclave/Network DAA SIPRNet Email Address: _____
Enclave/Network DAA NIPRNet (Unclassified) Email Address: _____
Technical POC and Phone Number:

_____

Technical POC SIPRNet E-mail Address:

_____

Technical POC NIPRNet (Unclassified) E-mail Address:

_____

Administrative POC and Phone Number:

_____

Administrative POC SIPRNet Email:

_____

Administrative POC NIPRNet (Unclassified) Email Address:

_____

Fax Number (Secure and Unsecure):

_____

System or Network Name: _____ *Premise Router IP Address:* _____
Network IP Address Ranges: _____

_____

_____ _____

_____

Rel IP Address Range(s) (if applicable): _____

_____

This form is to be submitted with all initial requests for DOD, Non DOD, Contractor, & Foreign National connections, including exercise and tactical connections. Additionally, this form is to be re-accomplished when there is a change to the approved configuration, certification, and/or a change that affects the answers on file.

Circle responses below.

Combatant Command, Service, or DOD Agency Sponsor/Joint Staff Validation/OSD Approval

(Mandatory for Foreign National, Contractor, and Non-DoD Activities

#1 Yes No Does this connection support a Non-DoD, Contractor, Foreign National User Connection or Cross Domain Solution (CDS)?

(Reference CJCSI 6211.02B, Appendix D to Enclosure C – If "YES", the sponsoring agency must submit a requirement letter to Joint Staff, J-6, for validation and OSD approval. A copy of the JS validation and OSD approval must be provided to the SCAO with the SIPRNet Connection Approval Process package.)

#2 Yes No N/A Has the Combatant Command, Service or DoD Agency submitted a sponsorship letter to the Joint Staff (J6T) requesting access to the SIPRNet?

(If yes, a copy of the sponsor's memorandum request must be provided to the SCAO with the SIPRNet Connection Approval Process package.)

#3 Yes No N/A Have the Joint Staff (J6) validated and OSD approved the request for SIPRNet/DATMS-C Access/ Connectivity?

Non-DoD Facility Access & Connections

#4 Yes No Do uncleared individuals have physical access to Non-DoD facility areas where work centers, terminals, or equipment connect directly or indirectly to the SIPRNet?

(Example: If Non-DoD personnel, either in support of a Non-DoD Government contract or maintenance support, to include cleaning people, have access to areas where SIPRNet workstations are located, a Yes response is required)

Contractor Facility Access & Connections

#5 Yes No Do uncleared contractors **have physical access to areas** where workstations are **connected directly or indirectly** to the SIPRNet?

(Example: If uncleared contractor personnel, either in support of a Government contract or maintenance support, to include cleaning people, have access to areas where SIPRNet workstations are located, a Yes response is required)

#6 Yes No Are cleared contractors at a non-DoD facility **users** on workstations **connected directly or indirectly** to the SIPRNet? Contract Number(s):

_____.

(Example: Any contractor (Prime or Sub) at a non-DoD facility (including Contractor facilities) that connects to the SIPRNet or on a separate network such as an Educational Facility that is logically or physically connected/interfaced to the users network, a Yes response is required.)

#7 Yes No Reference question #6. Are there any uncleared personnel providing support under this contract?

(Example: Any contractor personnel (Prime or Sub) that are providing administrative, logistical or services in support of the contract identified in number 6, a Yes response is required.)

Foreign National Access

#8 Yes No Do Foreign Nationals, to include Liaison Officers (Foreign nationals in US positions), **have physical access to areas** where workstations **connect directly or indirectly** to the SIPRNet?

(Example: If other than US personnel have access (escorted or unescorted) to the SIPRNet workstation areas, a Yes response is required.)

#9 Yes No Are Foreign Nationals, to include Liaison Officers, **users** on workstations on a network or subnet **connected directly or indirectly** to the SIPRNet?

(Example: If other than US personnel have user accounts on SIPRNet workstations or via a REL implementation configuration, a Yes response is required.)

DoD Facility Access & Connections

#10 Yes No Do Non-DoD individuals have physical access to facility areas where work centers, terminals, or equipment connect directly or indirectly to the SIPRNet?

(Example: If Non-DoD personnel, either in support of a DoD Government contract or maintenance support, to include cleaning people, have access to areas where SIPRNet workstations are located, a Yes response is required)

#11 Yes No Do uncleared individuals have physical access to facility areas where work centers, terminals, or equipment connect directly or indirectly to the SIPRNet?

(Example: If uncleared personnel, either in support of a DoD Government contract or maintenance support, to include cleaning people, have access to areas where SIPRNet workstations are located, a Yes response is required)

Network Connectivity

#12 Yes No Is the activity's SIPRNet network, to include subnet(s) and workstation(s), physically/logically connected or interfaced to a network or platform operating at any level other than Secret US Only? This includes tunneling, switches, or connections **with or without high assurance guards** in place? Include the Cross Domain Solution (CDS) Ticket Number (if Applicable) : _____

(Example: If a network is operating at Unclassified But Sensitive, Unclassified, Confidential, Top Secret, NATO Secret, REL, etc., has a physical or logical interface/connection with the SIPRNet, a Yes response is required. This includes configurations where the other network is cryptographically isolated (i.e., tunneled, GRE))

#13 Yes No Is the activity's SIPRNet network, to include subnet(s) and workstation(s), physically/logically connected or interfaced to a network or platform operating at another Secret US Level? This includes tunneling, switches, or connections **with or without high assurance guards** in place? Include the Cross Domain Solution (CDS) Ticket Number (if Applicable) : _____

(Example: If a network operating at Secret Level, e.g., SDREN, JTEN, DMON, etc., and has a physical or logical interface/connection with the SIPRNet, a Yes response is required. This includes configurations where the other network is cryptographically isolated (tunneled).)

Wireless Connectivity

#14 Yes No Does the activity's SIPRNet network configuration include wireless technology?

(Example: If wireless technology is/has been implemented on the users enclave the devices and configuration guidance must be included in the explanation.)

Ports & Protocol Registration

#15 Yes No Has the user registered all of the network systems on this connection with DOD Ports, Protocols and Services Management System, IAW DODI 8551.1?

(Explanation: All DISN activities are required to comply with this directive when connecting to a DOD network.)

If any of the above statements were answered with a **"YES"**, provide a **detailed** description of the systems involved, the security controls employed, information shared, allowed accesses, number of foreign nationals, etc. and identify the Designated Approval Authority for that connection. Please be sure to sign and include the reference number on any and all attachments. Any questions may be directed to DISA, SIPRNet Connection Approval Office (SCAO) at (703) 882-1455, DSN: 381-1455.

If this questionnaire and its attachments are classified after completion, please call the SCAO at DSN: 381-1455 to coordinate a secure fax transmittal. You may also return it by registered mail to the following address:

Defense Information Systems Agency
ATTN: GS213/SCAO
P.O. Box 4502
Arlington, VA 22204-4502

If the document and its attachments are unclassified after completion you may fax it to COMM (703) 882-2813 or DSN 381-2813.

CERTIFICATION: I certify that the information provided in this document and all attachments are accurate.

_____

Signature Block
Designated Approving Authority (DAA)