DEPARTMENT OF THE NAVY

DOD INFORMATION ASSURANCE CERTIFICATION AND ACCREDITATION PROCESS (DIACAP) HANDBOOK

Version 1.0

15 July 2008

DEPARTMENT OF THE NAVY

DOD INFORMATION ASSURANCE CERTIFICATION AND ACCREDITATION PROCESS (DIACAP) HANDBOOK

Version 1.0

Approved By

Date 7/16/08

Navy Operational Designated Accrediting Authority
Naval Network Warfare Command

Date 7/16/08

Marine Corps Designated Accrediting Authority
Headquarters Marine Corps
C4 - Information Assurance

DOCUMENT REVISION HISTORY

Version	Release Date	Summary of Changes
Version 1.0	July 15, 2008	Publish Version 1.0

TABLE OF CONTENTS

1.0 EXECUTIVE SUMMARY 1

2.0 INTRODUCTION 2

2.1 PURPOSE AND SCOPE 2
2.1.1 Purpose 2
2.1.2 Scope 3
2.1.3 Applicability 3
2.2 REFERENCES 4
2.3 DEFINITIONS 4
2.4 ACRONYMS 4

3.0 DON GUIDANCE ON C&A 5

4.0 C&A OVERVIEW 7

4.1 WHAT IS C&A 7
4.1.1 Certification 8
4.1.2 Accreditation 8
4.2 Categories of C&A 9
4.2.1 System Accreditations 9
4.3 Elements of C&A 16
4.3.1 Information Assurance Controls 17
4.3.2 Inheritance 17
4.3.3 How We Manage Risk 22
4.3.4 C&A Life Cycle in the Acquisition Process 25
4.3.5 C&A Maintenance 26
4.4 C&A Documentation 27
4.4.1 The DIACAP C&A Package 27
4.4.2 Comprehensive C&A Package Components and Related Activities 28

5.0 ROLES AND RESPONSIBILITIES 42

5.1 DEPARTMENT OF THE NAVY CHIEF INFORMATION OFFICER (DON CIO) 42
5.2 DON Senior Information Assurance Officer (SIAO) 42
5.2.1 SIAO Definition 42
5.2.2 SIAO Accountability 43
5.2.3 SIAO Responsibilities 43
5.3 Chief of Naval Operations (CNO) and the Commandant of the Marine Corps (CMC) 44
5.4 DON Deputy CIOs 44
5.5 Designated Accrediting Authority (DAA) 45
5.5.1 Introduction 45
5.5.2 DAA Definition 45
5.5.3 DAA Security Investigation, Position Designation, and Clearance Requirements 45
5.5.4 DAA Responsibilities 45

5.5.5 Operational DAA/MCEN DAA 46
5.5.6 Deployed DAA 46
5.5.7 Developmental DAA (DDAA) 47
5.5.8 Multiple Accreditors 47
5.6 Certifying Authority (CA) 48
5.6.1 Introduction 48
5.6.2 CA Definition 48
5.6.3 CA Security Investigation, Position Designation, and Clearance Requirements 48
5.6.4 Certifying Authority (CA) Responsibilities 48
5.7 Validator 49
5.7.1 Introduction 49
5.7.2 Validator Definition 49
5.7.3 Validator Security Investigation, Position Designation, and Clearance Requirements 49
5.7.4 Validator Accountability 50
5.7.5 Validator Responsibilities 50
5.8 Program Manager (PM) 50
5.8.1 PM Definition 50
5.8.2 PM Responsibilities 50
5.8.3 PM Accountability 51
5.8.4 System Owner (SO) 51
5.8.5 Information System Security Engineer (ISSE) 51
5.8.6 Information Assurance Manager (IAM) 52
5.8.7 Information Assurance Officer (IAO) 53
5.8.8 Introduction 53
5.8.9 IAO Accountability 53
5.8.10 IAO Definition 53
5.8.11 IAO Responsibilities 53
5.9 User Representatives (UR) 55

6.0 DON DIACAP 56

6.1 Overview 57
6.2 Activity 1 - Initiate and Plan IA C&A 58
6.2.1 Initiate DIACAP Package 60
6.2.2 Assign IACs and Other Requirements 64
6.2.3 Complete and Submit the DIP 67
6.2.4 DIP Review and Concurrence 69
6.3 Activity 2 - Implement and Validate Assigned IACs 70
6.3.1 Execute DIP and Conduct Testing 71
6.3.2 Compile the Test Results 80
6.3.3 Develop an IT Security POA&M 82
6.3.4 Complete the C&A Package 83
6.3.5 Echelon II/MSC Concurrence of C&A Package 86
6.4 Make Certification Determination and Accreditation Decision 86
6.4.1 CA Makes the Certification Determination 88
6.4.2 DAA Issues Accreditation Decision 89

6.5 Maintain Authorization to Operate and Conduct Reviews 91
6.5.1 Install Program/System 93
6.5.2 Maintain Situational Awareness 98
6.5.3 Conduct Annual Reviews 101
6.6 DECOMMISSION 102

ENCLOSURE (1) REFERENCES 105
ENCLOSURE (2) DEFINITIONS 110
ENCLOSURE (3) ACRONYMS 126
ENCLOSURE (4) LIST OF C&A PACKAGE COMPONENTS 130
ENCLOSURE (5) EXAMPLE OF SYSTEM IDENTIFICATION PROFILE (SIP) TEMPLATE 131
ENCLOSURE (6) EXAMPLE OF C&A PLAN 138
ENCLOSURE (7) EXAMPLE OF IAC IMPLEMENTATION PLAN 147
ENCLOSURE (8) EXAMPLE OF VALIDATION PLAN AND PROCEDURES 148
ENCLOSURE (9) EXAMPLE OF DIP CONCURRENCE SHEET TEMPLATE 149
ENCLOSURE (10) EXAMPLE OF C&A PACKAGE SIGNATURE PAGE TEMPLATE 150
ENCLOSURE (11) EXAMPLE OF DIACAP SCORECARD TEMPLATE 151
ENCLOSURE (12) EXAMPLE OF ACCREDITATION DECISION 154
ENCLOSURE (13) EXAMPLE OF ACCREDITATION LETTER 156
ENCLOSURE (14) EXAMPLE OF IT SECURITY POA&M TEMPLATE 158
ENCLOSURE (15) EXAMPLE OF STATEMENT OF COMPLIANCE 162

LIST OF FIGURES

Figure 1. System Accreditation Model 10
Figure 2. Type Accreditation Model 11
Figure 3. Site Accreditation Model 15
Figure 4. Simple Inheritance 18
Figure 5. Example of IAC Inheritance 19
Figure 6. Inheritance Hierarchy 21
Figure 7. DIACAP and the Acquisition Process 26
Figure 8. IAC's Structure 31
Figure 9. DoD DIACAP Cycle Overview 56
Figure 10. DIACAP Activities 58
Figure 11. Activity 1 – Initiate and Plan IA C&A 59
Figure 12. Activity 2 – Implement & Validate Assigned IACs 71
Figure 13. Activity 3 – Make Certification Determination and Accreditation Decision 87
Figure 14. Activity 4 – Maintain Authority to Operate and Conduct Reviews 92
Figure 15. Activity 5 – Decommission 102

LIST OF TABLES

Table 1. Risk Management Activities 23

1.0 EXECUTIVE SUMMARY

Information Assurance (IA) is the cornerstone in providing a secure, interoperable, net-centric Information Management (IM)/Information Technology (IT) environment across the Department of the Navy (DON) Enterprise. The confidentiality, integrity, availability, and technical superiority of DON information and Information Systems (ISs) are critical to maintaining our maritime dominance and national security. The Department of Defense (DoD) Information Assurance Certification and Accreditation (C&A) Process (DIACAP) evaluates the defense-in-depth layering of IA principles and controls that apply to people, processes, and technology, to ensure that they provide adequate protection for our information assets.

On 28 November 2007, DoD issued DoDI 8510.01, the DIACAP. This instruction directed the DoD to "begin an immediate transition to a streamlined and modern Certification and Accreditation (C&A) process that complies with the Federal Information Security Management Act (FISMA), of the E-Government Act of 2002, and is more compatible with the Department's IA control-based approach for information security and lends itself to the use of evolving automated C&A tools."

The DIACAP is a mechanism for negotiating IA requirements and capabilities between DoD IS and their supporting enclaves. It embraces a risk management approach that balances the importance of the information and supporting technologies to DoD missions against documented threats and vulnerabilities, the trustworthiness of users and interconnecting systems, and the effectiveness of IA solutions. DIACAP also considers the impact of impairment or destruction of the system, and the cost effectiveness of countermeasures. The DON implementation of DIACAP ensures compliance with this philosophy as well as DON, DoD, National Institute of Standards and Technology (NIST), Office of Management and Budget (OMB) and Federal standards, laws, regulations, directives, instructions and guidance. The DON DIACAP program defines the process and procedures that ensure adequate IS Information Assurance Controls (IACs) are implemented and tested, that any remaining risks are assessed and evaluated before accrediting the IS, and that security plans are continuously maintained and monitored for their effectiveness.

This handbook details the baseline DON approach to the DIACAP and the procedures necessary to obtain an accreditation decision for DON ISs undergoing the C&A actions as required under federal law, DoD and DON regulations and directives. In addition to this handbook, service unique guidance will be provided. DON ISs include all IT, applications, networks, circuits, enclaves, sites, infrastructure, and environments.

2.0 INTRODUCTION

The goal of net-centricity across the DoD elevated the importance of IA in order to facilitate assured information sharing, enhanced situational awareness, accelerated decision making, and improved joint warfighting, and necessitates the ability to dynamically exchange system-security credentials. Although C&A has long been considered an acceptable systematic means of addressing IA, existing C&A processes are no longer sufficiently flexible to address the dynamic security exchange requirements of the Global Information Grid (GIG) and its Navy instantiation, FORCEnet.

The evolution of IA C&A and the advent of enterprise-level drivers resulted in the DIACAP. The establishment of DIACAP addresses the continuing evolution of IT, and the way the DoD acquires, implements, operates and uses IT to comply with current and emerging federal requirements and guidelines. The benefits of this new C&A process include less time, effort and resources to implement, clear accountability, and reporting of the security status.

DIACAP contains the DoD processes for identifying, implementing, validating, certifying, and managing IA measures and services, expressed as Information Assurance Controls (IACs), and authorizing the operation of DoD ISs in accordance with statutory, Federal and DoD requirements. The DIACAP is a comprehensive C&A process that supports and complements the net-centric GIG-based environment.

This handbook provides the foundation for a comprehensive and uniform guide for executing the C&A process within the DON and all subordinate commands, bases, ships, organizations, and units. The DON C&A process applies to all DON ISs, IT applications, networks, circuits, enclaves, sites, and environments seeking C&A.

This handbook establishes a standard process for:

- Identifying, implementing, and validating standardized IACs.
- Authorizing the operation of DON ISs.
- Managing an IA posture throughout the DON IS's life cycle.

This handbook provides guidance for establishing a standard process for DON organizations and commands by defining a set of activities, general tasks, and a management structure to certify and accredit DON ISs. When properly executed, this process will help maintain the IA and security posture of an IS, IT applications, networks, circuits, enclaves, sites, infrastructure, and environments.

2.1 PURPOSE AND SCOPE

2.1.1 Purpose

This handbook defines the DON approach to implementing DIACAP procedures and documentation. Further, it defines the applicability, why C&A is important, and how C&A maps to an IS's life cycle. This handbook identifies the roles and responsibilities of key players,

explains the different types of C&A recommendations and decisions, and describes the activities and process steps that comprise the DIACAP.

2.1.2 Scope

The DIACAP is the overarching C&A process for the DoD. This handbook provides overarching guidance of the DON's implementation of DIACAP. Navy and Marine Corps may provide service-unique amplification to successfully execute these processes while maintaining the intent of DIACAP as set forth in this handbook. The Marine Corps amplification is contained in the USMC C4 IA Enterprise Directive on Certification and Accreditation.

The methodology defined in this handbook will result in a standardized C&A program across the DON that is in compliance with the DoD policy. Proper use of the C&A methodology will assure DON leadership that an appropriate level of security is implemented, sufficient controls are in place to adequately protect assets, and the ISs are operating at an acceptable level of residual risk.

The DON implementation of DIACAP provides visibility into the implementation of IA capabilities and services throughout the C&A process, facilitates collaboration among the stakeholders, and speeds the decision to authorize the operation of a given IS.

2.1.3 Applicability

C&A applies to the acquisition, operation, and sustainment of any DON IS, application, network, circuit, enclave, site, infrastructure, or environment that receives, processes, stores, displays, or transmits unclassified or classified information throughout the entire system life cycle (SLC), regardless of classification or sensitivity.

The DON DIACAP is applicable to all commands, bases, ships, organizations, and units that own and operate ISs within the DON.

2.1.3.1 This handbook is provided to support:

- The Office of the Secretary of the Navy, the Navy, the Marine Corps, and all other organizational entities within the DON, including the operating forces and supporting establishment.
- All DON owned or controlled ISs. This includes the development of new systems, the incorporation of systems into an existing infrastructure, the incorporation of systems outside the infrastructure, the development and testing of prototype systems, and the reconfiguration or upgrade of existing systems. Specific examples include but are not limited to:
  - DON ISs that support special environments as supplemented by the special needs of the program.
  - Platform IT interconnections (e.g., interfaces from weapons systems, sensors, medical technologies, or utility distribution systems) to external networks.
  - ISs under contract to the DON.

- Outsourced information-based processes, such as those supporting e-Business or e-Commerce functions.
- 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 that may be developed.
- DON ISs that are prototypes or Advanced Concept Technology Demonstrations (ACTDs).

2.1.3.2 Intelligence Systems

This handbook does not apply to IT systems processing Sensitive Compartmented Information (SCI), Nuclear Command and Control Extremely Sensitive Information (NC2-ESI), and Special Access Program (SAP) information. These systems are accredited separately by their respective communities under other procedures, policies, and authorities.

Nothing in this handbook shall alter or supersede the existing authorities and policies of the Director of Central Intelligence (DCI) regarding the protection of SCI and SAP for intelligence, as directed by Executive Order (E.O.) 12333 (see Reference (j)), and other laws and regulations. The application of the provisions and procedures of this handbook to SCI or other intelligence ISs is to address areas not otherwise specifically addressed. Users with these types of systems should contact the appropriate IA program office.

2.2 REFERENCES

Enclosure (1)

2.3 DEFINITIONS

Enclosure (2)

2.4 ACRONYMS

Enclosure (3)

3.0 DON GUIDANCE ON C&A

Information and resources are appropriately safeguarded at all times by implementing defense-in-depth mechanisms across the DON and DoD. IACs are employed in such a manner that information and resources are provided with the appropriate level of security commensurate with mission criticality, level of effort, and classification or sensitivity level of information received, processed, stored, displayed or transmitted. The process that verifies compliance with IACs, assesses their effectiveness, and evaluates the risk of operating an IS is called C&A. Per the DoDI 8510.01:

- The Navy and Marine Corps shall certify and accredit ISs through an enterprise process as defined in DIACAP to identify, implement, and manage IA capabilities and services. The DON shall establish and use a DIACAP-based service enterprise decision structure for DON C&A process as described in this handbook.
- The DON implementation of the DIACAP 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 that is consistent with the DIACAP.
  - Managing and disseminating service enterprise standards for IA design, implementation, configuration, validation, operational sustainment, and reporting.
  - Accommodating diverse ISs operating in multiple environments.
- All DON-owned, controlled or supported ISs shall be under the governance of the DON IA program. The DON IA program shall be the primary means for ensuring enterprise visibility and synchronization of the DIACAP compliance. Automated solutions for DIACAP will be responsible for providing this visibility.
- All DON ISs shall be implemented using the baseline DoD IACs in accordance with Reference (e). The baseline DoD IACs may be augmented or tailored if required to address localized threats or vulnerabilities.
- A DIACAP Scorecard reflecting the results of independent testing of the implementation of the required IA baseline controls, additional controls as required by the environment, and inherited/inheritance IACs that may be required by the DoD/DON or local requirements shall be made visible to the DoD Chief Information Officer (CIO) and to the DON Chief Information Officer (DON CIO).
- The C&A status of all DON ISs shall be made available to support the service operational DAA accreditation decisions.
- The implementation of IACs shall ensure that the controls identified by the DoD DIACAP Technical Advisory Group (TAG) as requiring annual review will be accomplished. The Navy and Marine Corps may provide service unique additional annual review requirements. Marine Corps amplification is contained in the USMC C4IA Enterprise Directive on C&A.

- Resources for implementing the DIACAP requirements shall be identified and allocated as part of the Defense Planning, Programming, Budgeting, and Execution (PPBE) process.
- Provisions for implementing the DON DIACAP requirements shall be written into contracts of systems, services and programs that are required to comply with the DIACAP. Failure to add appropriate requirements into contracts for IT systems does not provide justification for the lack of DIACAP compliance. All systems, services and programs will be required to comply with DIACAP, per reference (c).

4.0 C&A OVERVIEW

4.1 WHAT IS C&A

Understanding C&A begins with the recognition of the ever-present threat to US Federal and DoD IT assets and information. A threat is any circumstance or event with the potential to adversely impact an IS through unauthorized access, destruction, disclosure, modification of data, and/or denial of service. Threats can come from a variety of places and can be classified in a variety of ways including natural vs. man-made, internal vs. external, and intentional vs. unintentional. For example, threats can be:

- Unauthorized access to the network through any perimeter protections.
- Natural disaster, such as a hurricane, tornado, or earthquake damaging or destroying a facility.
- An accident or error made by an authorized user that could compromise classified or sensitive information or inadvertently (or intentionally) corrupt or destroy a file.
- Environmental inadequacies, such as power failures or insufficient humidity control.

Vulnerabilities, on the other hand, are the circumstances or conditions which may enable a threat to actually cause damage to an IS. Vulnerabilities can come in a variety of forms, including software coding errors or bugs, deficiencies in the environment such as no back-up power supply, inadequate fire suppression or physical security measures, or insufficient organizational policies or procedures such as inadequate user controls or back-up procedures. The combination of threats and vulnerabilities constitutes the risk faced by an IS. IACs are designed and implemented to reduce risk by reducing vulnerabilities, thereby minimizing exposure to threats. Realistically, however, all risk cannot be eliminated and the residual risk that remains after implementing IACs must be evaluated to determine if it is at an acceptable level. C&A is the standard DoD approach for identifying information security requirements, providing security solutions, and managing the security of DoD information systems. C&A provides standardization, increased confidence, lower level of risk, and reduced overall cost. System Owners (SOs) are to align the process with the program strategy and integrate the process activities into the system life cycle.

The key to the C&A process is the coordination between the primary stakeholders of the system, comprised of the IT PM or System Manager (SM) or SO, Echelon II Representative, Major Subordinate Command (MSC), the DAA, the Certifying Authority (CA), and the User Representative (UR). These stakeholders resolve critical schedule, budget, security, functionality, and performance issues. This collaborative effort is documented in a package that is used to determine the system risk. The term “stakeholders” used throughout this handbook is meant to include the parties mentioned above as a minimum; others may be added as needed, based on the unique nature of a given system, to create the body of interested parties to collaboratively resolve issues as they arise and at key points throughout the process.

4.1.1 Certification

Certification is the comprehensive evaluation of the technical and non-technical security safeguards of an IS to support the accreditation process that establishes the extent to which a particular design and implementation meets a set of specified security requirements. The CA performs a comprehensive evaluation and validation of a DoD IS, establishing the degree to which it complies with assigned IAC based on standardized procedures. This comprehensive evaluation includes an examination of the threats to the system and the data that resides on it and both the security functions (i.e., technical features) of an IT system and the assurances that those functions are correctly implemented when deployed to a specified environment.

The CA issues a statement regarding the extent to which an IS/component complies with the IACs and the level of residual risk involved in operating the system.

A certification statement is normally required for an accreditation decision, but does not allow a system to connect to an operational network. In order for a system to be operationally deployed, it must receive an accreditation approval from the DAA.

4.1.2 Accreditation

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. Accreditation ensures that unacceptable risk is not introduced into operational networks and systems. The DAA issues an accreditation decision for the IS based upon the certification statement provided by the CA and an assessment of the impact to the GIG. An accreditation decision normally requires a certification determination, unless unusual circumstances (such as operational need time factors) drive a DAA-only assessment leading to an accreditation decision. These are extremely rare occasions, and some collaboration between the DAA and CA would still likely occur. In addition to the specific information provided by the CA, the DAA takes into consideration the need for the system to execute DON missions, current threat levels, and the overarching security posture of the GIG.

The accreditation decision applies to an instance of a DON IS ready to operate as a stand-alone entity or connect to an operational network, or when systems require re-accreditation. The accreditation decision is a balance of mission or business need, protection of personally identifiable information (PII), protection of the information being processed, and protection of the information environment, and thus, by extension, protection of other missions or business functions reliant upon the shared information environment.

Accreditation decisions are expressed as Authorization to Operate (ATO), Interim Authorization to Operate (IATO), Interim Authorization to Test (IATT), or Denial of Authorization to Operate (DATO). Absent an accreditation decision, a system is considered unaccredited and therefore is not approved to operate.

4.2 Categories of C&A

For IA purposes, all DON C&A packages are categorized and managed as being in one of two categories: system or site. Within the DON, these categories are further subdivided into additional subcategories.

A system accreditation evaluates a particular system, i.e., hardware, software, and firmware. The System C&A categories include:

- Systems.
  - Proof of Concept
  - Prototype
  - Locally acquired systems
  - Joint systems (or non-DON systems)
- Type certifications and accreditations: instances where a single system is distributed or installed in a number of different locations.
- Platform IT interconnections.
- Simple or closed networks.
- Outsourced IT-based processes.

A site accreditation evaluates the environment in which applications and systems are installed. The Site C&A category include:

- Enclaves.
- Complex or enterprise networks.
- Sites such as local area networks (LANs), commands, and unique geographic locations.

This allows for the C&A package to be categorized according to the accreditation being sought and determines the process steps to be completed in the DIACAP cycle of activities.

4.2.1 System Accreditations

A system accreditation includes the certification and accreditation of a single instance of a specifically configured system for a particular physical/operational environment, see Figure 1. It may be as simple as a single software application or as complex as a large combination of hardware and software. Typically, the system will be defined by the components required to support its functionality. System accreditations are considered the default and are not usually labeled specifically as system accreditations.

An accreditation package is considered to be a system accreditation unless otherwise noted. This category also includes the C&A of proof of concept systems, prototype systems, locally acquired systems, and joint systems. Proof of concept and prototype systems are typically originated and developed in the Research, Development, Test, and Evaluation (RDT&E)

environment, but may need to be temporarily installed in an operational environment to validate their feasibility. In this case, an IATT must be issued for a specified duration covering the test period and the system will be de-installed upon the expiration date of the IATT.

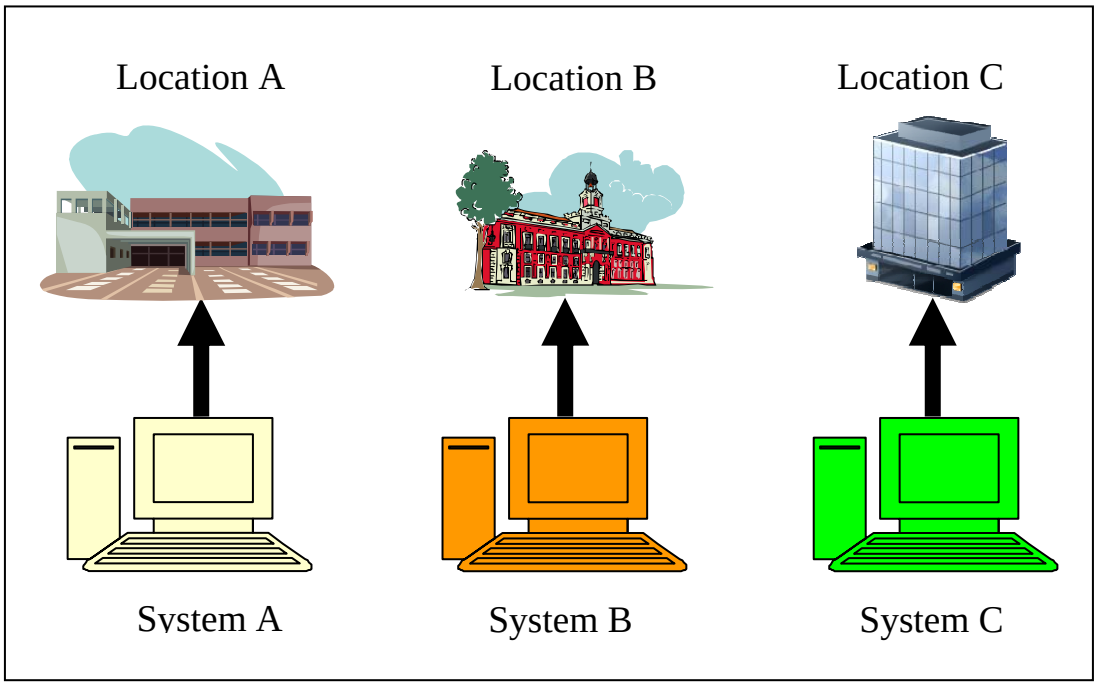


Figure 1. System Accreditation Model

4.2.1.1 Type Accreditations

In some situations, a system consisting of a common set of hardware, software, and firmware is intended for installation at multiple locations, see Figure 2. A type accreditation satisfies the C&A requirements in this case by obtaining a single accreditation that permits installation of multiple instances of this specifically configured system in a particular physical/operational environment at multiple locations. Rather than testing and validating the system IACs at every site where it is needed, the type accreditations allow for the installation of identical systems based on the validation of all the IACs at **one** representative site. If the IT system will be installed in multiple environments/enclaves/enterprises, such as the Navy Marine Corps Internet (NMCI), OCONUS Navy Enterprise Network (ONE-Net), etc., then the IACs must be validated in one representative site for each of the identified environments. Installation environments must be described in detail and connections to enclaves noted.

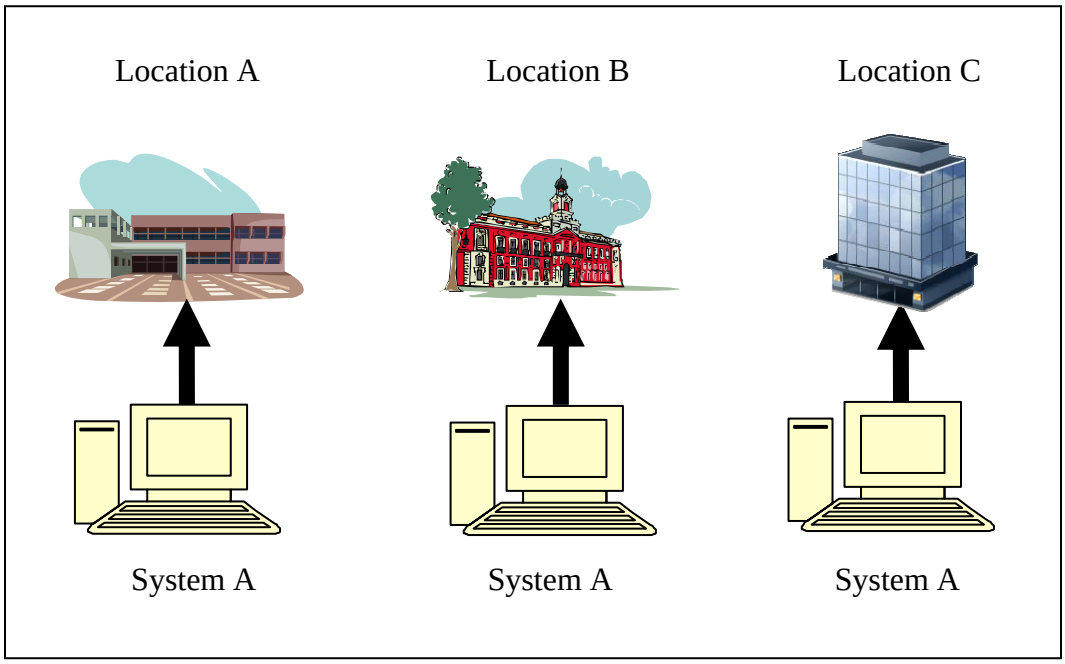


Figure 2. Type Accreditation Model

The PM/system owner/system acquisition entity is responsible for determining if a type accreditation is desired. If the goal is to obtain type accreditation for the system, the initial type accreditation requires satisfaction of all applicable IACs, including design, configurable, and environmental/non-technical controls. The responsibility also includes the identification of any IACs which are not applicable or must be inherited from a hosting facility or site. This part includes a validation test in the developmental (lab) environment to ensure that all applicable IACs are validated. The type accreditation C&A package is submitted through the C&A process with the specific goal of obtaining a type accreditation.

- Design controls are those IACs that describe features built into the system. Because they are built in and do not change, they are only tested once.
- Configurable controls are those IACs pertaining to technical features that depend on proper system configuration. Because they are configurable, if the system is to be operated in both a laboratory and an operational environment, they must be tested in both places to ensure configuration compliance, or the laboratory must exactly duplicate the operational environment. An example is password complexity. Over time, the rules associated with the complexity of a user account password may change. Although the current rule requires that a certain combination of upper case, lower case, numeric, and non-numeric characters be part of a minimum password, it may change tomorrow based upon a change in policy. The IAC to ensure that password complexity is compliant with policy does not change, but the configuration that determines what is tested and what constitutes a pass/fail do change.
- Environmental/non-technical controls are those IACs inherited from the environment(s) into which the system is installed. Because these controls are not present in a laboratory environment, they are only tested in the operational environment.

In the accreditation documentation, the DAA ensures that a statement of residual risk is included that clearly defines the intended operating environment for the major application or general support system. The DAA also identifies specific uses of the application or system and operational constraints and procedures under which the application or system may operate.

A system granted type accreditation, when installed in the operational environment, must satisfy all applicable IACs. Design controls were satisfied when the type accreditation was granted, and do not need to be tested again. Configurable and environmental/non-technical IACs must be validated for each installation of the system. In general, environmental/non-technical IA Control satisfaction may be inherited from the site. The site is responsible for validating the correct implementation of the configurable and environmental/non-technical IACs based on the PMs provided Validation Plan and Procedures. Once the installed system completes validation, documentation is forwarded to the CA and DAA to complete the accreditation of the installation.

Because type accredited systems rely on IACs that are inherited from the environment, only accredited sites may host type accredited systems. Accredited systems are not to be installed at sites that are not accredited.

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 validation activities because the local organization is provided with the type accreditation documentation that specifies the configurable and environmental/non-technical (inherited) IACs.

4.2.1.2 Platform IT Interconnections

A platform IT interconnection is a physical or logical connection at or crossing the boundary between a platform IT system and a non-platform IT system. Platform IT interconnection has readily identifiable security considerations and needs that must be addressed in both acquisition and operations. Examples of platform IT interconnections include communication interfaces for data exchanges with enclaves for mission planning or execution, remote administration, and remote upgrade or reconfiguration. Platform IT Interconnection accreditation requests must be identified as such. A Memorandum of Agreement (MOA) may be required between the platform IT owner and the enclave owner to ensure that adequate security measures are in place.

When platform IT interconnects with external networks in order to exchange information, the interconnections must be certified and accredited to ensure that the information exchange is protected. If not already established as part of the interconnection negotiation, the platform is required to identify the Mission Assurance Category (MAC) and Confidentiality Level (CL) of its interconnecting IT. The connecting enclave must meet or exceed the MAC and CL of the interconnecting platform IT. If the MAC or CL of the platform IT is lower than that of the connecting enclave, the enclave is responsible for ensuring that the enclave integrity, availability, and confidentiality are not degraded by the interconnection. The enclave is also responsible for providing any additional measures required to extend IA services, such as identification and authentication to the platform IT during the interconnection, and to protect the platform IT from interconnection risk, such as unauthorized access.

4.2.1.3 Simple or Closed Network Certifications and Accreditations

Under System Accreditation, a simple or closed network accreditation includes the certification and accreditation of a collection of interconnected nodes. A network is considered simple when it is single-mission, small in nature, and/or standalone. A closed network is defined as a network system that is "closed loop" or is standalone and has no external connections to the internet, GIG, or other environments. Examples of a simple or closed network system are some RDT&E networks or lab networks, test networks, etc.

A network system is based on a coherent security architecture and design. The network environment includes the physical environment, administrative environment, and the communication relationship with other ISs. Network accreditation is a single accreditation of more than one IS component under the control of an operational DAA. Network accreditation combines the system-specific information from the components on that network into an integrated C&A package describing the network with its components, as well as the IACs common to the domain of that network.

4.2.1.4 Outsourced IT-Based Processes Certifications and Accreditations

An outsourced IT-based process is a general term used to refer to outsourced business processes supported by private sector IS, outsourced information technologies, or outsourced information services. An outsourced IT-based process performs clearly defined functions for which security considerations and needs are readily identifiable and addressed in both acquisition and operations. Outsourced IT-based processes may provide functionality associated with an application, enclave, platform IT, or some combination. If the outsourced IT-based process is effectively a DoD enclave, i.e., if it is established only for DoD purposes, is dedicated to DoD processing, and is under DoD configuration control (e.g., the Defense Logistics Agency (DLA) Business Systems Modernization Production Center or NMCI), it should be managed and reported, certified, and accredited as a DoD enclave.

If, however, it supports non-DoD users or processes and is not under DoD configuration control, it must be managed and reported as an outsourced IT-based process. Confidentiality, availability, integrity, authentication, and non-repudiation requirements for DoD information in an outsourced environment are determined by its mission assurance category, confidentiality or sensitivity level, and need-to-know. Technical security and generation of the required C&A documentation for the outsourced environment are the responsibility of the service provider. Outsourced applications that are accessed by DoD users within DoD enclaves (e.g., PowerTrack) are subject to DoD enclave boundary defense controls for incoming traffic (e.g., ports and protocols and mobile code). Responsibility for procedural and administrative security is shared between the service provider and the supported DoD entity. Security roles and responsibilities are to be made explicit in the acquisition, along with the performance and service-level parameters by which the DoD will measure the IA profile of the outsourced IT-based process.

The DoD categorizes commercial connections/networks as outsourced IT-based processes. These are special cases that must be appropriately managed. Examples of these include the Navy Public Affairs Office needing access through a commercial Internet Service Provider (ISP) to gain access to public social networks, e.g., MySpace, that have been restricted at the .mil

domain, or Naval law enforcement needing access to sites where their military address may draw adverse attention and compromise a particular case. In both examples, the local Navy or Marine Corps unit would need to prepare accreditation documentation that provides evidence that the connection operates under the appropriate IACs and does not introduce risk to the environment. Note: All connections via commercial ISPs require a waiver through DISA. Specific instructions on this process may be obtained in Appendix D to Enclosure (C) of CJCSI 6211.02B of 31 July 2003, see Reference (oo).

4.2.1.5 Enclaves Certifications and Accreditations

An enclave is a collection of computing environments connected by one or more internal networks under the control of a single authority and security policy, including personnel and physical security. Enclaves are a grouping of systems based on a physical characteristic such as location or connectivity. Enclaves provide standard IA capabilities such as boundary defense, incident detection and response, and key management, and also deliver common applications such as office automation and electronic mail. Enclaves may be specific to an organization or a mission, and the computing environments may be organized by physical proximity or by function independent of location. Enclaves always assume the highest MAC and CL of the Automated Information System (AIS) applications or outsourced IT-based processes they support, and derive their security needs from those systems. An enclave MAC and CL remain fixed during interconnection to other enclaves; they do not inflate to match the MAC or CL of an interconnecting enclave. Enclaves with higher MACs connecting to enclaves with lower MACs are responsible for ensuring that the connection does not degrade its confidentiality, availability or integrity.

4.2.1.6 Complex or Enterprise Network Certifications and Accreditations

Under site accreditation, a Complex or Enterprise Network Accreditation includes the C&A of a collection of interconnected nodes. Complex or Enterprise Networks are relatively large, multiple-mission, and complex in nature with external connections to other networks and enclaves. Examples of these kinds of networks are enterprise networks, such as the NMCI, ONE-Net, Marine Corps Tactical Network (MCTN), etc.

An Enterprise Network system is based on a coherent security architecture and design. The network environment includes the physical, administrative, and communication relationships with other networks. Network accreditation is a single accreditation of more than one IS component under the control of an operational DAA. Network accreditation combines the system-specific information from the components on that network into an integrated C&A package describing that network as well as the security controls common to the domain of that network.

4.2.1.7 Site Certifications and Accreditations

A site is the total computing environment that automated ISs, networks, or components operate. The environment includes physical, administrative, and personnel procedures as well as communication and networking relationships with other ISs. Site accreditation is a single accreditation of one or more enclaves, networks, etc. under the control and responsibility of an

Information Assurance Manager (IAM). A site may include more than one facility or location (e.g., building or base) provided that those locations are under the accrediting authority of the same operational DAA for that site. A site accreditation consolidates the individual system-specific information from the different C&A packages at that site into a single integrated C&A package describing that site as well as the security controls common to the domains at that site.

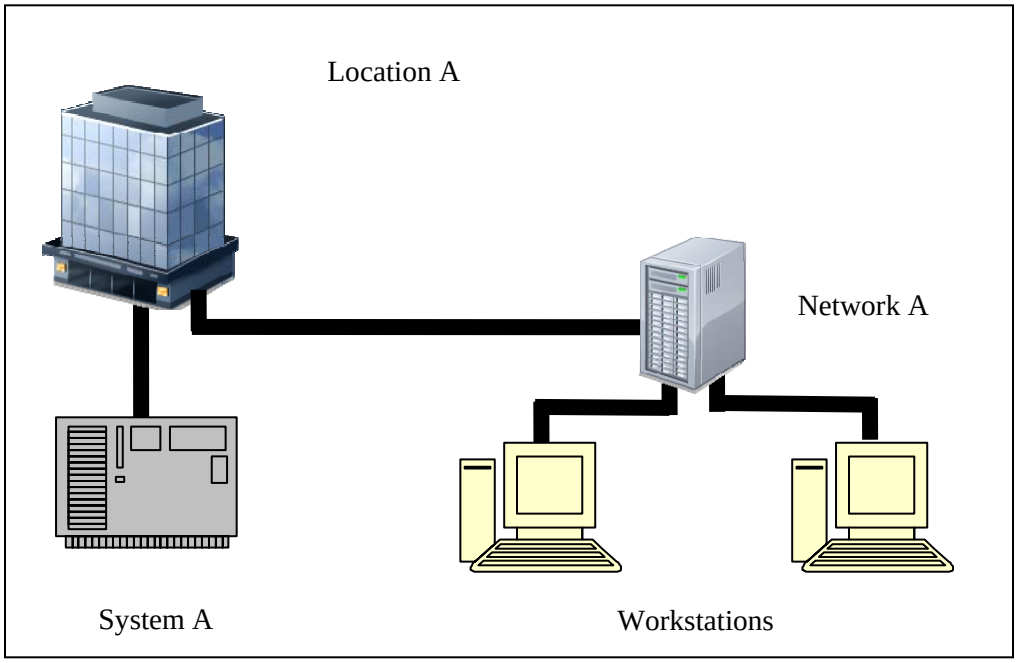


Figure 3. Site Accreditation Model

A site consists of one or more security domains, which are logical groupings of systems based on a common security policy. Sites may have additional security domains containing other classifications and/or coalition partner information. Each security domain contains one or more enclaves. Enclaves are characterized by their membership in a security domain. When multiple confidentiality levels (CLs) are present in a single package, such as when classified and unclassified systems or networks are combined in a single package, different IACs must be carefully applied and documented for each of the different CLs. IAMs should consider providing separate documentation for each security domain to clearly define applicability for IACs and simplify the evaluation process.

A site may identify inheritable IACs for an IS being installed or hosted at that site and which therefore requires accreditation. Site accreditation ensures that these environmental IACs are, in fact, provided to the ISs being installed, that additional risk is not being introduced by the installed systems, and that risk is not being introduced by the site into the IS being installed or hosted. When a type-accredited system or hosted application is integrated into an accredited site, the site accreditation package is updated to reflect the installation of the system or hosted application.

Each operational IS under the accrediting authority of a DAA must be accredited. Site accreditations eliminate the administrative burden of individually accrediting each system or enclave. The IAM is to determine whether systems will be accredited individually, as an enclave system, or as a site based on the local environment or conditions.

If the IAM has multiple groupings of systems that logically create a "Site" (i.e. classification) or the IAM has responsibility for multiple geographical sites, the IAM determines how many site accreditations will be performed and which automated ISs (AISs) will be contained in each site accreditation. For example, the IAM may choose to separately accredit groups of enclaves based on their classification. Alternatively, all the enclaves at a site (regardless of classification) could be in a single site accreditation.

The IAM, working in conjunction with the Information Assurance Officers (IAOs), will consolidate the data associated with the threats, vulnerabilities and risks previously identified for the individual systems and enclaves as well as the IACs required by all ISs and/or enclaves. The IAM will identify the mission risk associated with the vulnerabilities in the site operational environment and identify any countermeasures furnished by characteristics of the site that mitigate the risk to the identified enclave(s). The IAM will identify and assess any operational impact of proposed countermeasures to the operational mission capability and will provide a statement to the CA and DAA. The DAA will render an accreditation decision based on this information and the DAA's assessment of its operational impact on the GIG.

The allocation of AISs to site accreditations is typically determined by the dynamics of the enclaves and the classification of the accreditation documents. If one enclave, such as a laboratory, is constantly changing its components and configuration, it may be simpler to accredit that enclave separately from the rest of the site, as an enclave (system) which has a more static configuration. If the site has enclaves at different classifications, it may be more practical to have a site accreditation for each security classification and thereby allow information sharing among the individuals cleared to a level commensurate with their enclaves.

The Site IAM ensures that the site operation of the IS is accomplished in accordance with the site accreditation approval package. The site certification validates that the operational procedures for the IT, environmental concerns, and physical security pose no unacceptable risks to the information being processed. The site accreditation provides authorization to operate the IS at that site as described in the C&A package under an acceptable level of risk. Where an IS may not be confined to a fixed site (i.e., tactical or mobile systems and embedded systems in aircraft), the IS may be examined in representative sites or environments.

4.3 Elements of C&A

The C&A process ensures that adequate security measures are in place to protect the information that resides on the DON networks. This process is applicable to all DON systems under development and those already in production. The application of DIACAP achieves the following:

- Validates security requirements established for a system or network.

- Examines implemented safeguards to determine if they satisfy DON security requirements and identifies any inadequacies.
- Obtains management approval to authorize initial or continued operations of the system or network.

The following specific tasks and activities within the C&A process are critical to ensuring that DON IA program objectives are fully aligned with DoD policies and standards, and cannot be stressed enough.

4.3.1 Information Assurance Controls

This section contains information extracted from DoDI 8500.2, Reference (e).

An IAC is an objective IA condition of integrity, availability, and/or confidentiality achieved through the application of specific safeguards or through the regulation of specific activities expressed in a specified format (i.e., a control number, a control name, control text, and a control class). The objective condition is testable, compliance is measurable, and the activities required to validate the IAC are assignable, and are thus accountable. Specific management, personnel, operational, and technical controls that span acquisition, proper security engineering, connection management, and IA administration are applied to each DoD IS registered with the DON IA program and made visible to the DON CIO.

Compliance with a baseline set of IACs is required for each IS and establishes a standard minimum level of IA for all DoD IS. The baseline set of IACs is assigned according to MAC and CL. MACs and CLs are independent; that is, a MAC I system may process public information and a MAC III system may process classified information.

Nine combinations of MAC and CL are possible. For each combination of MAC and CL, the baseline IACs and the appropriate test and evaluation procedures for each IAC are specified as a baseline set. Testers validate each IAC's compliance through the successful execution of one or more specific validation test procedures for that IAC. For the Navy, this baseline listing of IACs and their associated validation test procedures can be accessed at this link: https://www.fleetforces.navy.mil/netwarcom/navycanda/default.aspx. The Marine Corps uses Xacta which automatically assigns IA controls based on MAC and CL levels. Xacta can be accessed at: https://hqtelosweb.hqmc.usmc.mil/

4.3.2 Inheritance

A key component of inheritance is the requirement for the DIACAP team to obtain agreement on the controls that will be inherited by the individual system. The remainder of this section provides a comprehensive description of inheritance to familiarize the DIACAP team with the concept.

One of the basic concepts of the DIACAP is inheritance; however, this is not a new concept. Figure 4 illustrates the basic concept of inheritance, which is that ISs can inherit an IAC and its compliance or non-compliance from their local environment when they do not have the capability to organically supply the functionality that would produce IAC compliance. While the concept appears simple, applying inheritance in the C&A process can potentially be quite

complex. The process by which IACs are inherited, declared inheritable, certified, and accredited, and the documentation of that parent and child relationship, is called inheritance. This section of the handbook explains the fundamentals of these relationships and how they apply in the DIACAP.

There are four principles in the DIACAP that are essential to the inheritance concept:

- For inheritance purposes there are only two types of entities, systems (i.e., applications, clients/server systems, networks, etc.) and groupings of systems (such as sites, enclaves, environments, etc.).
- Accredited systems can only be placed in accredited systems or sites.
- Accredited systems or sites can only accept accredited systems.
- Sites and Enclaves are convenient aggregations of separate ISs.

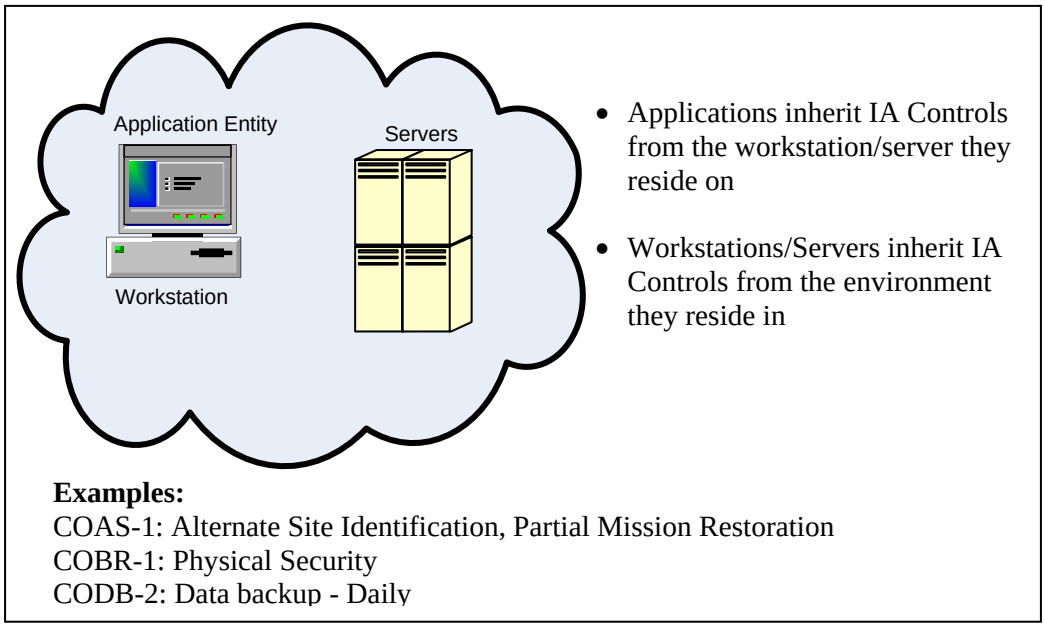


Figure 4. Simple Inheritance

These simple principles are the foundation for inheritance. C&A is the entire process of evaluating the risk in an IS, weighing the residual risk after mitigation against the operational needs, and authorizing this IS to operate. As networks and systems get more and more numerous, interconnected and complex, not every IS needs to satisfy every IAC independently. This does not mean that a particular IAC is not met, but rather that the IS (child) can rely on a system or grouping of systems up the hierarchy, i.e. a parent IS, site or enclave, to supply the IAC compliance that the child system does not or can not satisfy directly. In order to certify and accredit an IS, an understanding is needed of which IACs will be satisfied directly by the child IS and which IACs will be satisfied by inheritance through the parent systems/sites/enclaves that are part of the environment in which the child IS resides. Fundamentally:

- Inheritance is the process in which external IACs are either used (inherited) or made available (inheritable) for others to use to satisfy the compliance requirements for that IAC.
- Inherited and inheritable IACs must be identified and the relationship between systems using them must be established, documented and maintained.
- Inherited controls are IACs that a child IS "inherits" from a parent system, site or enclave to satisfy that control.
- Inheritable controls are those controls that an accredited system or site offers or supplies to a child system to satisfy an IAC security requirement.

The benefits of inheritance come from the elimination of duplication of effort and testing. Sharing an IAC's compliance status and its associated evidence allows C&A practitioners to model an environment where security mechanisms are shared across multiple ISs. Inheritance eliminates testing redundancy by passing the actual results, associated validation artifacts, and compliance status from the parent IS to each inheriting IS. Validation test results and supporting documentation are maintained by the parent IS and are made available to PM/SOs of receiving ISs upon request.

An example of an IAC inheritance is illustrated in Figure 5:

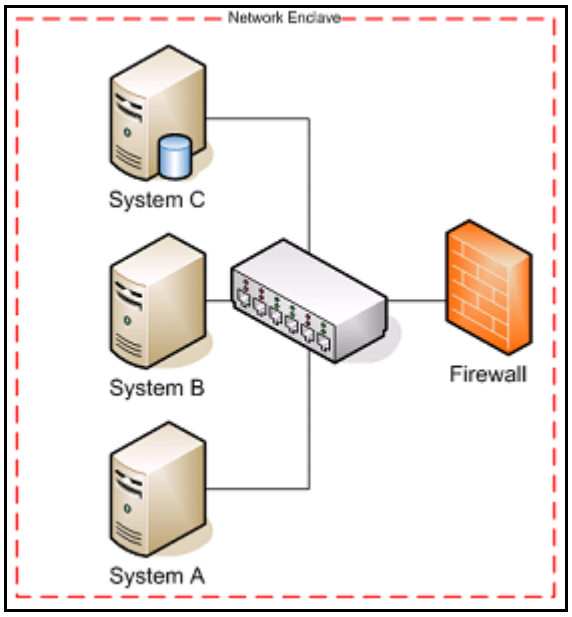


Figure 5. Example of IAC Inheritance

A network enclave hosts three systems: System A, System B and System C. A firewall that sits inside of the secure network environment provides protection to all three systems. The DIP and DIACAP Scorecard for the network enclave reflect the Boundary Defense IAC, EBBD-2, which is satisfied in part by the firewall. The network enclave DIP also designates this control as inheritable.

Systems A, B and C inherit IAC EBBD-2, and document this relationship on their respective DIP, Scorecard, and IT Security Plan Of Actions & Milestones (IT Security POA&M) (if necessary). All status data, test results, and supporting material associated with EBBD-2 are passed from the network enclave to the three systems dynamically, and when changes occur.

Inheritance is a two way street. When an IS inherits an IAC, it uses the compliance status of the inherited IAC as if it was its own. This means that, when the inherited IAC has been correctly implemented, the IS uses this inheritance relationship to satisfy the IAC security requirement. When the inherited IAC is not compliant, the inherited relationships bring the risk from this non-compliant IAC to the IS inheriting it. While it does not make sense to plan on inheriting a non-compliant IAC, this situation can occur when an inherited IAC becomes non-compliant. The IAC must be compliant in order for an IS to inherit the functionality that satisfies the security requirement. When an inherited IAC is or becomes non-compliant, the IS must then provide the functionality to comply with an IAC. If the environment doesn't supply a compliant IAC, an item must be added to the IT Security POA&M as a non-compliant IAC.

Inheriting the security provided by an IAC that has been satisfied can potentially become complex. To further illustrate some of the complexities that exist in implementing inheritance, consider Figure 6 where the Wizbang Information System (Wiz IS) is operating attached to a hierarchy of networks.

- The Wiz IS consists of one server, the server's specifically configured Operating System, and the three FAM approved COTS software packages of Microsoft Word, Excel, and PowerPoint.
- The Wiz IS resides on a Local Area Network (LAN) in Building 99 on the Base Timbuktu.
- The Building 99 LAN, in turn, is part of the Timbuktu Base Area Network (BAN).
- The Timbuktu BAN, in turn, is part of the Somewhere Metropolitan Area Network (MAN).
- The Somewhere MAN is part of the Somewhere Region (SR) Wide Area Network (WAN).
- The SR WAN is part of the Naval CONUS Enterprise Network (eNET).

Each one of these networks is, in it own right, an IS, and it can be accurately referred to as a system versus a network. The Somewhere MAN network is an IS that consists of an orderly arrangement of routers, switches, firewalls, etc. designed to fulfill a specific mission and provide specific services to multiple BAN Systems. On the other hand, with the exception of the Wiz IS, all of these network systems can also be referred to as Enclaves according to the definition of an enclave in Enclosure (2).

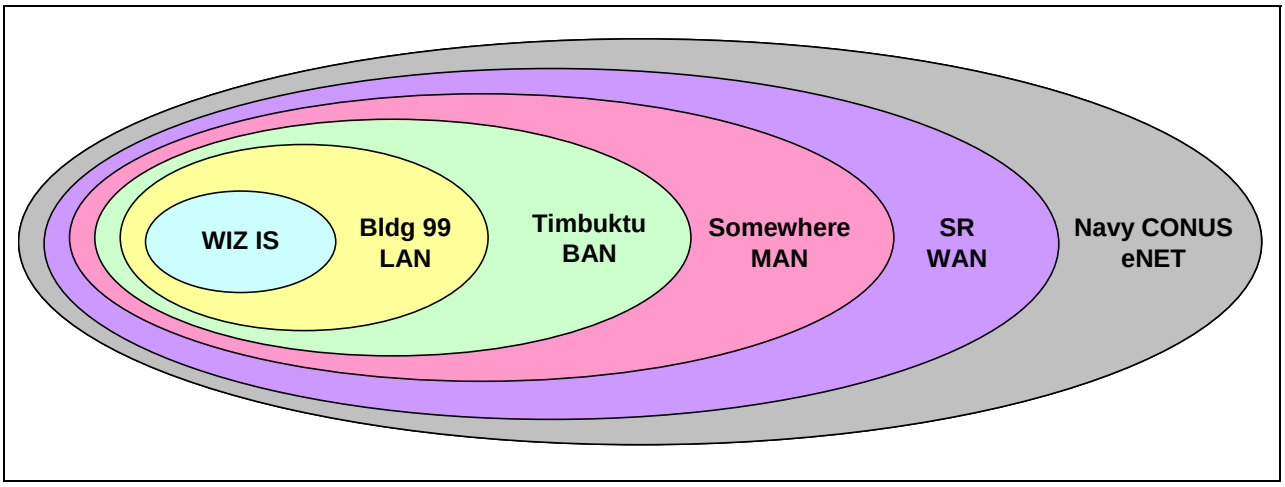


Figure 6. Inheritance Hierarchy

This concept illustrates the following:

- All IT networks can be referred to as either Systems or Sites/Enclaves.
- A site (from the IA perspective) is a collection of one or more ISs coupled with the site's geographically based Physical Security System of locks, guards, badges, etc.

When viewed from this perspective, inheritance of security (satisfied IACs) or inheritance of risk (when any inherited IACs become non-compliant) always occurs between ISs or between an IS and a collection of ISs referred to as a site or enclave. The distinction depends upon the accreditation status and accreditation boundary of the system/site/enclave under consideration for inheritance. Obviously, a security feature or risk can't be inherited from an unaccredited system/site/enclave. Further, some IACs may be more accurately evaluated and accredited at one level of the hierarchy of systems than at another.

Consider the "Navy CONUS eNET" in the example above. It is perfectly reasonable to identify, evaluate, and accredit the programmatic IACs (i.e. software development, configuration control board, etc.) and those technical IACs that relate to Firewall, Intrusion Detection/Prevention System, Server Farm, etc. (sub-systems) in a Type Accreditation of the "eNET" Architecture system. In this example, the "Timbuktu BAN" enclave can inherit IACs from the Somewhere MAN to satisfy functionality that it can't provide itself. The Timbuktu BAN in turn, can provide these inheritable IACs to the Bldg 99 LAN as if the Timbuktu BAN had the functionality as its own. However, in doing so, the Timbuktu BAN incurs the obligation to monitor the status of these inherited IACs (from the Somewhere MAN) to ensure that they remain in compliance, and if a change occurs where they become non-compliant, they must work with the Somewhere MAN to resolve the issues and notify the Bldg 99 LAN of the events.

It is this "collection of multiple systems/sites/enclaves" concept that makes inheritance complex. This is because each individual inheritance "link" must be specifically identified in an accreditation package. Inheritance of security or risk ***is totally dependent*** upon how those other IS/sites/enclaves are defined, how they interface with a particular IS, their accreditation

boundary, and their current accreditation status. Inheritance is simple if all the interfaces and all the security features and risk associated with the other ISs/sites/enclaves are known. Inheritance is complex if these pieces aren't known. Fortunately, the systems/sites/enclaves that offer inheritable IACs must be accredited, and determining what security/risk they provide can be determined by "following the data flow". Therefore, when deciding which IACs are inheritable by another system "lower" in the hierarchy (child system) or inherited from another system "higher" in the hierarchy (parent system), a complete understanding of the data flow and interfaces between ISs/sites/enclaves as well as the security/risk features provided by those ISs/sites/enclaves is required.

The C&A process described in this handbook details how the IACs for an IS are identified, how these IACs are designated as being met by the IS directly, or whether they will be inherited from a parent IS/site/enclave or will be inheritable by child ISs further down the hierarchy.

4.3.3 How We Manage Risk

Risk assessment is central to the risk management process. To ensure a common understanding of risk assessment, the DON has adopted a standard approach to evaluating risk. This standard approach will enable reciprocity between the Services in understanding and accepting risk assessments and accreditations. This risk assessment methodology is derived from Federal, DoD, and DON policies; incorporates industry best practices; and provides a standardized, systematic, and analytical approach to assessing the risks associated with a system, regardless of its life-cycle stage.

Every DON IS C&A package includes a risk assessment in the system security documentation. Once the necessary IACs are implemented, a risk management review (or risk assessment) is conducted to determine the level of operational risk. Once accredited, IAM's must ensure that systems and networks are being maintained at an acceptable level of risk. The risk management review assesses the system vulnerabilities with respect to the documented threat, ease of exploitation, potential rewards, and probability of occurrence. The operational procedures and safeguards (security controls), as well as system and network security design features are evaluated to determine their effectiveness and ability to offset risk.

There are two primary methods that can be employed to conduct risk assessment: qualitative and quantitative. The risk assessment process employed in the DON is qualitative, as the parameters involved in the risk assessment often cannot be strictly defined. As such, the DON risk assessment process relies on the expertise and judgment of the personnel performing the task. When quantifiable information is available, such as the likelihood of a component failure or the facilities flooding, quantitative risk analysis techniques may also be used, to supplement the qualitative process.

4.3.3.1 Risk Management Activities

Operational requirements and resource constraints make it impractical to protect every system against all possible threats. However, losses can be controlled by applying risk management throughout the system life cycle. The system life cycle is typically defined as having five stages, shown in Table 1. During each life cycle phase, the risk management process assists system

developers and users in making informed decisions affecting the system security posture in both its current life cycle phase and subsequent ones. The C&A process both supports and is supported by risk management activity. The interdependence of these IA components is shown in Table 1 and is discussed in the paragraphs that follow.

System Life Cycle Phase	C&A Life Cycle Phase	Risk Management Activity
Concept Definition and Design	Initiate and Plan IA C&A	Identify system security requirements and strategy for protecting the system through its life.
Development and Integration	Implement and Validate Assigned IACs	Evaluate trade-offs between functional and security requirements and document the decisions which are made.
Installation and Operation	Make Certification Determination and Accreditation Decision	Conduct a risk assessment to validate that both system and security requirements are met within the anticipated operational environment.
Maintenance	Maintain Accreditation	Assess the effect that time and/or changes to the system have on the information environment security and identify actions required to maintain acceptable levels of risk.
Disposal	Decommission the IS	The IS is removed from operation and a number of IA-related events are required relative to the disposition of DIACAP registration information and system-related data or objects in supporting IA infrastructures and core enterprise services.

Table 1. Risk Management Activities

Under DIACAP, documenting the system begins during the Concept and Design stage to ensure that all information is maintained from system design inception through disposal. During the Concept and Design stage, risk management helps identify system security requirements and the strategy for protecting the system through its life. In the Development and Integration stage, risk management is used to evaluate trade-offs between functional and security requirements. As a system progresses to the Installation and Operation stage, risk management validates that both system and security requirements are met within the anticipated operational environment. After a system becomes operational (Maintenance stage), the personnel responsible for the system exercise risk management to assess how time and/or changes have impacted the system and to identify actions required to maintain acceptable levels of risk.

4.3.3.2 Comprehensive Risk Evaluation

A comprehensive evaluation examines all elements of the system and its intended operational environment. The first step in risk evaluation is system characterization. In order to understand what threats may exist, the functionality of the system and characteristics related to its mission must be examined. This is why the accreditation request must include essential elements such as mission description, concept of operations (CONOPS) summary, system architecture diagram along with hardware and software lists, and operating and computing environment in the C&A package.

Once the system characteristics are understood, the next step in risk evaluation is threat identification. Circumstances or events that could potentially cause harm to, or reduce the effectiveness of, the system or any of its essential elements should be documented in a threat analysis. Threats may be natural, human, or environmental. The threat analysis should include an estimation of the motivation, resources, and capabilities required for successful exploitation and an estimate of the likelihood of occurrence.

The next step in risk evaluation is to identify the vulnerabilities of the system. Vulnerability is a weakness in the system that could be exploited either accidentally or intentionally. Vulnerabilities will be identified during Validation testing for compliance with applicable IA Controls, wherein the security functions (i.e., the security behavior) of a system and the assurances that those functions are correctly implemented are examined. IA Controls that pass validation testing in accordance with DOD 8500.2 and 8510.01 will be considered at an acceptable level of level of risk. All IA Controls or other security requirements that fail validation testing will be consider weaknesses in the system or network and must undergo additional risk assessment. If the system has not yet attained the stage in the life cycle where official testing is performed, vulnerabilities can be identified by analysis of the system architecture, potential threats, security advisories from government and vendor sources, and other useful sources, such as the World Wide Web.

With the system characterization, the threat analysis, and the vulnerability identification, risk analysis can be accomplished. During risk analysis, combinations of threats and vulnerabilities are scrutinized for likelihood of exploitation and the magnitude of impact successful exploitation could have on the mission and national security. Important factors in this assessment are the criticality of the system and its data, availability of resources and motivation of threat agents, potential impact to the availability, integrity and confidentiality of the system and its data, and any mitigating factors that might repel or prevent a threat agent from action.

There are three primary elements of the DoD and DON risk assessment process. These are IA Control validations results, Impact Codes, and Severity Categories. Validation results show security strengths and highlight IA Control weaknesses. IA Control weaknesses are considered potential risks and further risk assessment is required. Impact codes are an assessment of the magnitude of network-wide consequences of a failed IAC and apply equally to validated and failed IA Controls. Only those Impact Codes for IA Controls that failed validation testing are used in the risk assessment process.

In support of the finalization of the risk assessment process, severity categories are utilized to identify the severity of risk of the failed IA Control weaknesses by the CA after comprehensive evaluation of all mitigations, system design and network security features. Security Categories constitute the CA's determination of the residual risk of the IA Controls, system or network.

4.3.4 C&A Life Cycle in the Acquisition Process

DIACAP is a cycle of activities that are performed iteratively throughout a system's life cycle, beginning with acquisition and continuing through decommissioning. Where in the C&A cycle a given system currently is will determine what activities must be performed. Continual evaluation of IAC compliance, annual review, and reaccreditation requirements will require multiple iterations of the DIACAP activities over the life cycle of the system. DIACAP has been designed to foster addressing the security concerns early in the acquisition process for a system. To be most effective, IACs must be considered, designed and integrated into a new system from inception and should be closely tied to acquisition milestones. Various C&A activities are performed during the development stages of a system to ensure that appropriate IACs are properly designed, integrated, and implemented to facilitate adequate security for the system or application.

This starts with the first C&A milestone of registering the system with the DON IA program. The next C&A milestone is achieving concurrence on what IACs are required and how they will be tested. The IACs are then developed with the system, tested, and the results are documented and submitted in the complete C&A package for certification and accreditation early in the system's developmental timeline, allowing for the IA concerns to be properly addressed during development. Finally, the issuance of the accreditation giving the system the authority to operate or test while connected to an accredited environment. Figure 4 illustrates the relative timing of these C&A process steps, milestones, and where in the acquisition timeline they fall.

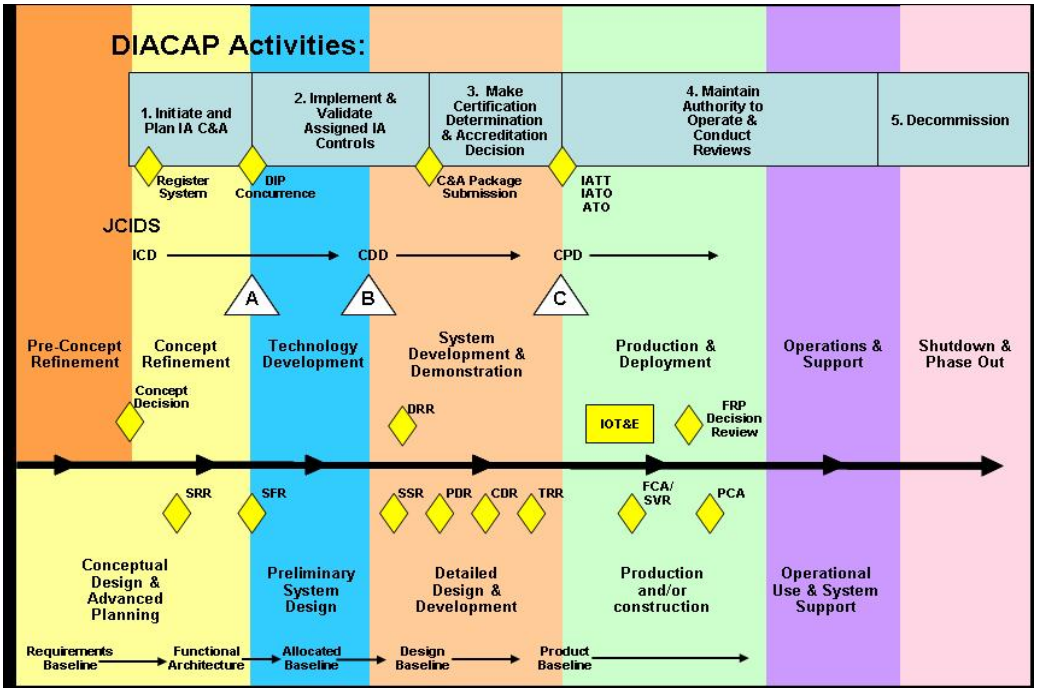


Figure 7. DIACAP and the Acquisition Process

Once deployed through the operational life of a system, IACs are continuously monitored for the impacts of any system change or upgrade, and for their effectiveness. Every functionality change or improvement to the system must be evaluated for its impact to the security integrity of the system. Evaluation activities must be performed in a continuing cycle until the system is de-installed or decommissioned.

For new systems, security accreditation must be scheduled for completion prior to operational deployment. The balance of the C&A activities and tasks to validate the correct implementation of all IACs must then be completed at each location where the system is installed. The system's program manager must also complete the various recurring C&A activities as changes are engineered or as the threats to or vulnerabilities of the system continue to evolve.

4.3.5 C&A Maintenance

Automated ISs, applications, and networks and the environments in which they operate are extremely dynamic and continuously evolve. Because threats to DoD ISs change, vulnerabilities in Commercial-Off-The-Shelf (COTS) and Government-Off-The-Shelf (GOTS) products are continuously discovered, and the intended deployment environments experience change, IACs must also evolve and must be continuously monitored in order to effectively mitigate any adverse impact these changes may have on the security integrity of the system. Since accreditation ensures that the system is being operated under an acceptable level of risk, the accreditation must be maintained. Continuous evaluation of the system following accreditation ensures that the system continues to operate under an acceptable level of risk. If at any time the

level of risk becomes unacceptable, the DAA can issue a DATO and the system must be de-installed or shut down until the risk has been mitigated back to an acceptable level and these mitigations are evaluated by the CA to be sufficiently effective. The CA's recommendation is then provided to the DAA and the system can be re-accredited.

4.4 C&A Documentation

DIACAP uses a data-driven approach as much as practical for C&A documentation. To standardize the way C&A activities are documented, reduce errors in packages, and, to the greatest extent possible, simplify the documentation process, a series of templates for entering data has been created. The DIACAP templates and examples can be found at these links:

For the Navy: https://www.fleetforces.navy.mil/netwarcom/navycanda/default.aspx.

For the Marine Corps: https://hqtelosweb.hqmc.usmc.mil/.

The DIACAP C&A package is intended to be a living document. Maintained electronically, it will be continuously updated throughout the life cycle of the system. For new systems being developed, this package will be created over an extended period of time due to the availability of information. Once filled in, the documents created from the templates will be updated as needed to reflect the security status of the system. The C&A package has two variants: the Comprehensive DIACAP C&A package containing the full set of documents, and the Executive C&A package.

4.4.1 The DIACAP C&A Package

The DIACAP C&A package is developed through DIACAP activities and maintained throughout a system's life cycle. Implementing the activities of the DIACAP is detailed in Section 6 of this handbook. These activities generate the C&A package components listed in the "Comprehensive Package", while the "Executive Package" contains a subset of the information contained in the "Comprehensive Package" necessary for an accreditation decision. The components that comprise the Comprehensive and Executive Packages are outlined below.

Additionally, acquisition contracts may specify additional IA C&A deliverables. Once the DON automated solution is implemented, specific components and supporting documentation linked to a C&A package will be available for review, based on user roles and access rights.

4.4.1.1 Comprehensive C&A Package

The Comprehensive C&A package includes the full set of templates, diagram, and supporting documentation necessary to describe the system or site and its compliance with all required IACs.

The Comprehensive Package includes the following components, along with their sub-components:

- SIP
- DIP
- Scorecard
- IT Security POA&M

4.4.1.2 Executive C&A Package

The Executive C&A package is a subset of the Comprehensive C&A package, and contains the key elements from the Comprehensive C&A package required for an accreditation decision. Service DAAs may request the Comprehensive C&A package versus the Executive C&A package when they determine that they need the additional elements contained in the Comprehensive C&A package for their decision.

The Executive C&A package contains, at a minimum, the following components:

- SIP
- Scorecard
- IT Security POA&M
- Any other documentation that the DAA determines relevant to making an accreditation decision

4.4.2 Comprehensive C&A Package Components and Related Activities

The following describes the major components that make up the Comprehensive C&A package, and identifies the related DIACAP activities that create, edit, modify, check, or complete a specific C&A document:

4.4.2.1 System Identification Profile (SIP)

The set of information gathered during system registration is referred to as the SIP, which becomes part of the DIACAP package for the IS, and is maintained throughout the system's life cycle. For new systems, not all the information required to complete the SIP will be available at the program's start, but this document will be updated as information does become available. The SIP must be completed prior to submitting the C&A package for certification. Registration is the activity where the DIACAP-related elements and system-unique attributes of the DON IS are made visible to the DoD Chief Information Officer (CIO)/Senior Information Assurance Officer (SIAO) and to the DON IA Program for the purpose of tracking management indicators (e.g., DIACAP status) and for FISMA reporting.

System registration establishes the relationship between the DON system or site and the governing DON Component IA program. The SIP identifies the minimum data requirements, plus explanations, for registering an IS with the Component. An overview of the type of

information included in the SIP can be seen in Enclosure (5). Registration involves recording descriptive system acquisition and IA data in a manner that allows unique system identification. Registration commences a dialog between the system owner and the DON Component CIO, which continues until the site or system is decommissioned. Typically, this information can be found in program/project documentation, such as the Initial Capabilities Document (ICD), system requirements/specifications, architecture and design documents, etc.

4.4.2.2 DIACAP Implementation Plan (DIP)

The DIP is a compilation of several documents that describe the overall system, the IACs, and how the IACs will be implemented and tested. The DIP is first developed as a draft, and then it is continually updated and refined throughout the C&A process as the various activities are completed. The DIP contains the current implementation status of IACs assigned/required for a system. This includes those IACs that will be inherited. The DIP is part of the DIACAP C&A package used by both the CA and the DAA for accreditation, and should be consistent with the program schedules.

The DIP contains the following components:

- C&A Plan
- IAC Implementation Plan
- Validation Plan and Procedures
  - ◊ Validation Results (Report)

4.4.2.3 C&A Plan

The C&A Plan is a sub-component of the DIP and provides details about the IS. It is made up of documents that capture the data required to make an accreditation decision. For a more detailed description of the essential elements in a C&A Plan, see templates and examples beginning with Enclosure (4).

The C&A Plan contains the following elements:

- Mission Description
- CONOPS Summary
- User Description and Clearances
- Operating and Computing Environment
- Physical Security Measures/Facility
- Threat Analysis
- Security Roles
- System Architecture Diagram
- Accreditation Boundary - Boundary Diagram MUST include:

- ◊ Buildings and Location
- ◊ Server Names
- ◊ IP Addresses
- ◊ Cross Domain Solutions
- ◊ Circuit Identifiers
- ◊ Routers
- ◊ Switches
- ◊ IA Equipment Providing Protection
- ◊ Any external interfaces other than the CCSD

- External Interfaces and Data Flow
- Hardware List
- Software List
- Ports, Protocols and Services (PPS) Listing
- C&A Tasks and Milestones
- Contingency Plan
  - ◊ Business Continuity Plan
  - ◊ Disaster Recovery Plan
  - ◊ Incident Response Plan

See Enclosure (6) for a more detailed description of the elements of the C&A Plan.

4.4.2.4 IAC Implementation Plan and the Validation Plan and Procedures Spreadsheet

Both the IAC Implementation Plan and the Validation Plan and Procedures are spreadsheet templates that are first downloaded and then customized by setting the MAC and CL for the IS.

The Defense IA program establishes the baseline set of IACs to be applied to all DoD ISs, as described in DoDI 8500.2. These IACs form a management framework for the allocation, monitoring, and regulation of IA resources that is consistent with Federal guidance provided in OMB A-130. Ultimately, IACs are intended for the enabling of IA across the dynamic environment of the Global Information Grid (GIG), and to support net-centricity.

IACs serve as a common management language for establishing IA needs and ensuring consistency. The DoD IACs establish a common dialogue among service components, information owners, PMs, outsourced service providers, enclave managers, IA certifying and accrediting authorities, and IS security engineers. They aid in the negotiation and allocation of IA requirements and capabilities, enable traceability to specific IA solutions, and provide a consistent reference for certification activities and findings.

The DoDI 8500.2 IACs are organized into eight subject areas, indicating the major subject or focus areas to which an individual IAC is assigned.

Each IAC is an objective IA condition of integrity, availability, or confidentiality achieved through the application of specific safeguards or through the regulation of specific activities that is expressed in a specified format. The objective condition described is testable, compliance is measurable, and the activities required to achieve the IAC are assignable and thus accountable. IACs are uniquely named and formally catalogued, and can therefore be referenced, measured, and reported against throughout the life cycle of a DoD IS.

An IAC is composed of the following elements:

- **IAC Subject Area -** One of eight groups indicating the major subject or focus area to which an individual IAC is assigned.

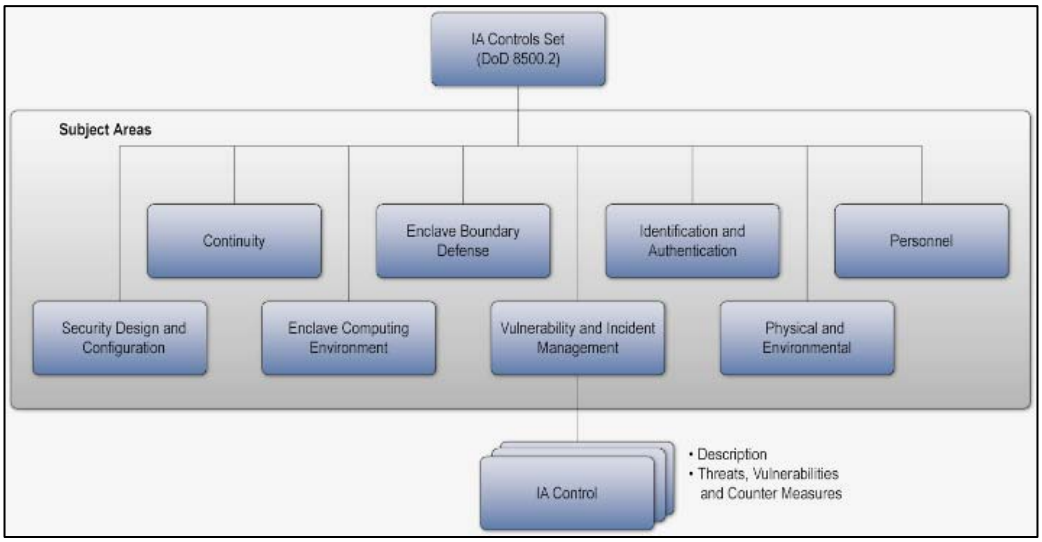


Figure 8. IAC's Structure

Abbreviation	Subject Area Name	Number of IACs in Subject Area
DC	Security Design & Configuration	31
IA	Identification and Authentication	9
EC	Enclave and Computing Environment	48
EB	Enclave Boundary Defense	8
PE	Physical and Environmental	27
PR	Personnel	7
CO	Continuity	24
VI	Vulnerability and Incident Management	3

- **IAC Name -** A brief title phrase that describes the individual IAC.
- **IAC Text -** One or more sentences that describe the IA condition or state that the IAC is intended to achieve.
- **IAC Number -** A unique identifier comprised of four letters, a dash, and a number. The first two letters are an abbreviation for the subject area name and the second two letters are an abbreviation for the individual IAC name. The number represents a level of robustness in ascending order that is relative to each IAC.

Specific IACs from the DoDI 8500.2 control set are captured in the DON set of templates, so that IACs are assigned and applied to each IS to achieve the enterprise baseline levels of availability, integrity, and confidentiality for the system's MAC and CL. Assignment of IACs is discussed under IACs Assignment.

4.4.2.5 Determining Applicable IACs for an IS

Identifying the baseline IACs that apply to a particular site or system is a critical DON DIACAP implementation activity. To execute this activity, an appropriate MAC and CL must be established for each IS. DoD Instruction 8500.2, "Information Assurance Implementation," identifies IAC sets applicable to a system specific MAC and CL designation. The DON CIO, DAA, or official DON Community of Interest (COI) representative may add additional IACs, to locally augment the security stringency of baseline control set, only when the augmented controls increase the security stringency established by the enterprise baseline IACs.

The following steps, and accompanying diagram, describe the IAC selection process and illustrate the steps in identifying the IACs applicable to your IS.

- Determine the IS type.
- Determine the MAC and CL for the IS.
- Determine the IACs baseline (based on MAC and CL).
- Augment the baseline with any DON Component-level or system-level IACs.

4.4.2.5.1 Determine the IS Type

The foundation of the DON IA management structure is composed of IA programs at the individual DON IS level. Determination of the IS type impacts IACs assigned to the system (e.g., stand-alone systems – a type of enclave), and who is responsible for maintaining those IACs (e.g., cases of Type Accreditations and Outsourced IT-Based Processes).

4.4.2.5.2 Determining the MAC and CL

After the IS type has been determined, define the MAC and CL for the system. DoDI 8500.2 defines three DoD mission assurance categories and three confidentiality levels to be applied to an IS. Together, the MAC and CL are used to determine which IACs are assigned and applied to

an IS to achieve the enterprise baseline levels of availability, integrity, and confidentiality for that MAC and CL. Use the following descriptions to determine the appropriate MAC and CL for an IS.

4.4.2.5.3 MAC

The MAC reflects the importance of information relative to the achievement of DoD goals and objectives, particularly the war fighters' combat mission. Mission assurance categories are primarily used to determine the requirements for availability and integrity. The Department of Defense has three defined MACs. Criteria for assignment of the MAC are described below:

- **Mission Assurance Category I (MAC I)**. 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 of a MAC I system are unacceptable and could include the immediate and sustained loss of mission effectiveness. MAC I systems require the most stringent protection measures.
- **Mission Assurance Category II (MAC II).** Systems handling information that is important to the support of deployed and contingency forces. The consequences of loss of integrity are unacceptable. Loss of availability is 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.
- **Mission Assurance Category III (MAC III).** Systems handling information that is necessary for conducting day-to-day business, but does not materially affect support to deployed or contingency forces in the short term. The 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.

4.4.2.5.4 Confidentiality Level (CL)

The CL is primarily used to establish acceptable access factors, such as requirements for individual security clearances or background investigations, access approvals, and need-to-know determinations; interconnection controls and approvals and acceptable methods by which users may access the system (e.g., intranet, Internet, wireless). The CL establishes security classification, sensitivity, and need-to-know requirements.

Criteria for assignment of the CL are:

- **Classified.** A DoD IS that processes Classified Information.
- **Sensitive.** A DoD IS that processes Sensitive Information. Sensitive Information is information the loss, misuse, unauthorized access to, or modification of which could

adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of title 5, United States Code, "The Privacy Act", but which has not been specifically authorized under criteria established by Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy. Examples of sensitive information include, but are not limited to, information in payroll, finance, logistics, and personnel management systems. See DoDI 8500.2 Enclosure (1) Reference (e) for further information and examples of sensitive information.

- **Public.** A DoD IS that processes Public Information. Public Information is Official DoD information that has been reviewed and approved for public release by the information owner in accordance with DoD Directive 5230.9.

4.4.2.5.5 Determining the IACs Baseline

Once the MAC and CL have been determined for the IS, the IACs baseline can be established. The IACs baseline for a given IS includes those IACs, from DoDI 8500.2, that are mandated based on the system's specific MAC and CL. This baseline establishes the mandated minimum level of security for an IS of a given MAC and CL.

The DON maintains the IAC Implementation Plan and the Validation Plan and Procedures Spreadsheets that contain the DoD required IACs. Additional information on MAC and CL can be found in the attached Enclosure (1) Reference (e).

4.4.2.5.6 Augment the baseline with any DON Component-level or system-level IACs

The baseline DoD IACs may be augmented, if required, to address additional threats or vulnerabilities.

A Mission Area (MA), DON Component, a Community of Interest (COI), or a local system can augment the baseline IACs with additional IACs to address special security needs or unique requirements of the ISs to which they apply. Augmenting IACs must neither contradict nor negate DoD baseline IACs, must not degrade interoperability across the DON Enterprise, and may not be used as a basis for denying connectivity of systems that have met the DoDI 8500.2 baseline IACs for MAC and CLs of the gaining IS. Procedures for implementing augmenting IACs are the responsibility of the originator.

Work with your MA, DON Component, and COI to determine what, if any, DON Component-level IACs have been developed for application to your site or system.

4.4.2.5.7 IACs Inheritance

Identifying specific IACs which are inheritable is primarily the responsibility of the site. There are limited instances in which a system may provide inheritable controls as well (e.g., Information Assurance Suite); when this is the case, the PM of the system is responsible for identifying the inheritable controls as well. Identification of inheritable controls that are actually inherited by a system is the responsibility of the PM which owns the system. The DIP of the system receiving inherited controls must identify which IACs are inherited and the site or other

system they are inherited from. Inherited IACs are also reflected on the DIACAP Scorecard of the receiving IS and are marked as being inherited. Inherited weaknesses must be reflected on the IT Security POA&M. See Section 4.3.2 for a more complete discussion of inheritance.

4.4.2.6 IACs Implementation Plan and Validation Plan and Procedures

The IACs Implementation Plan and Validation Plan and Procedures are sub-components to the DIP and are created and synchronized to the IACs contained in the Finalized IAC controls spreadsheet. These synchronized plans and procedures are used to implement and validate the assigned IACs.

The supporting documentation for certification includes the Validation Report containing the results of the independent validation, details of any artifacts associated with the implementation of IACs (e.g., Security Technical Implementation Guides (STIGs)), other implementation guidance, and various recommendation and concurrence letters.

4.4.2.6.1 Conduct Validation

Validation includes all tasks related to the execution of the Validation Procedures that are associated with assigned IACs. For each IAC, one or more Validation Procedures have been developed which describe requisite preparatory steps and conditions, actual validation steps and expected results. Each procedure includes associated supporting background material, sample results, or links to automated testing tools.

4.4.2.6.2 Validation Results (Report)

The validation results will be entered into the appropriate columns in the Validation Plan and Procedures spreadsheet.

The results of the validation activities conducted using the IACs Implementation Plan and the Validation Plan & Procedures are documented in the DIACAP Scorecard, and convey information on the IA posture of a site or system in a format that can be exchanged electronically. It documents the accreditation decision and must be signed, either manually or with a DoD PKI-certified digital signature. The DIACAP Scorecard contains a listing of all IACs and their status of Compliant, Non Compliant, or Not Applicable. The DIACAP Scorecard and explanations of the fields can be found in Enclosure (11).

Validation results are also recorded according to the criteria and protocols specified in each procedure and are made a permanent part of the C&A package, along with any artifacts produced during the validation (e.g., output from automated test tools or screen shots that depict aspects of system configuration). For inherited IACs, validation test results and supporting documentation are maintained by the originating IS and are made available to CAs of receiving ISs, by request.

Upon completion of the validation activities, an IT Security POA&M is initiated to document non-compliance results and non applicable IACs, if necessary. For any identified IA weakness, an associated Severity Category is assigned by the CA (and documented within the IT Security POA&M) to indicate the likelihood of the weakness being exploited.

4.4.2.7 DIACAP Scorecard

The DIACAP Scorecard is a summary report that succinctly conveys information on the IA posture of a site or system in a format that can be exchanged electronically. It documents the accreditation decision and must be signed, either manually or with a DoD PKI-certified digital signature. The DIACAP Scorecard contains a listing of all IACs and their status. A notional scorecard and explanations of the fields can be found in the appendices.

The status of actual results for all assigned Validation Procedures is compiled into a DIACAP Scorecard. The statuses of assigned IACs are indicated on the Scorecard as:

- **Compliant (C).** IACs for which expected results for all associated validation procedures have been achieved.
- **Non-Compliant (NC).** IACs for which one or more expected results for all associated validation procedures are not achieved. Not achieving expected results for all validation procedures does not necessarily equate to unacceptable risk.
- **Not Applicable (NA).** IACs that do not impact the security posture of the IS as determined by the DAA.

4.4.2.8 IT Security POA&M

An IT Security POA&M is used to identify tasks and corrective actions needed to maintain an accreditation. It specifies resources required to accomplish the elements of the plan, any milestones in meeting the task, and scheduled completion dates for the milestones. For any non-compliant IAC, the IT Security POA&M details the actions necessary, schedule, and milestones for reaching compliance with that control. The IT Security POA&M is a living document that is continuously updated during the accreditation life cycle of a system, program, or site. This is an important document for the CA and DAA to consider in developing their recommendations or decisions. In addition, program officials are required to update the DON CIO, through the Service DAAs, on their progress on at least a quarterly basis and at the direction of the CIO. This enables the CIO to monitor DON-wide remediation efforts and provide the DON's quarterly update to OMB.

The IT Security POA&M is a living document designed to assist agencies in closing their security performance gaps, assist inspectors general (IGs) in their evaluation work of agency security performance, and assist OMB with oversight responsibilities. The System level IT Security includes all IT security weaknesses found during any other review done by, for, or on behalf of the agency including, but not limited to, Government Accountability Office (GAO) audits, financial system audits, official security test and evaluation or compliance review, and critical infrastructure vulnerability assessments.

The purpose of an IT Security POA&M is to assist DON components in identifying, assessing, prioritizing, and monitoring security weaknesses found in programs and systems, along with the progress of corrective efforts for those vulnerabilities. OMB requires DoD Components to prepare IT Security POA&Ms for all programs and systems where an IT security weakness has been found.

The DON CIO, DON Deputy CIO (Navy), and DON Deputy CIO (Marine Corps) are responsible for maintaining the confidentiality of IT Security POA&Ms because they may contain pre-decisional budget information.

The IT Security POA&M addresses:

- Specific corrective actions necessary to demonstrate that all assigned IACs have been implemented correctly and are effective;
- The agreed-upon timeline for completing and validating corrective actions; and
- The resources necessary and available to properly complete the corrective actions. This section provides the instructions for filling out both the System Level IT Security POA&M and the Component Level IT Security POA&M.

IT Security POA&Ms are permanent records. Once posted, weakness will be updated, but not removed, after correction or mitigation actions are completed. The initial milestones and completion dates should be not altered. Missing milestone dates for FISMA reported systems by more than 90 days will require quarterly reporting to OMB and DoD and may include providing the IT Security POA&Ms to OMB. Inherited weaknesses are reflected on the IT Security POA&Ms. IT Security POA&Ms may be active or inactive throughout a system's life cycle as weaknesses are newly identified or closed.

The PM/SO or SM is responsible for implementing the corrective actions identified in the IT Security POA&Ms and, with the support and assistance of the IAM, provides visibility and status to the DAA. The Service DAAs are responsible for monitoring and tracking overall execution of system level IT Security POA&Ms and providing consolidated information to the DON Deputy CIO (Navy) and DON Deputy CIO (Marine Corps).

In order to reflect the complete IA posture of a DON IS in a single document, the IT Security POA&M is also used to document DAA-accepted Non-Compliant IACs and baseline IACs that are Not Applicable because of the nature of the system. See Enclosure (14) for the required IT Security POA&M format template.

4.4.2.9 Certification Recommendation

When the system has completed all implementation and validation tasks, the DIACAP Package is submitted to the CA for a certification determination. A CA representative is an active member of the DIACAP Team from inception and continuously assesses and guides the quality and completeness of DIACAP activities and tasks and the resulting artifacts.

Certification considers the IA posture of the DON IS itself, that is, the overall reliability and viability of the IS plus the acceptability of the implementation and performance of IA mechanisms or safeguards that are inherent in the system itself. The majority of this evidence comes from the implementation and validation evidence for the IACs. Each control is validated according to the requisite validation procedures, and the expected results compared to the actual results give the CA an indication of the compliance status for each IAC.

How the system behaves in the larger information environment provides visibility to situational awareness and assists in the determination of adequate network defense services. For example,

does the system introduce vulnerabilities to the environment or does it correctly and securely interact with information environment management and control services?

The certification determination is based on the actual validation results. It considers Impact Codes associated with IACs in a non-compliant status, associated Severity Categories, expected exposure time (i.e., the projected life of the system release or configuration minus the time to correct or mitigate the IA security weakness), and cost to correct or mitigate (e.g., dollars, functionality reductions). The weaknesses identified on the IT Security POA&M reflect residual risk to the system.

As part of the certification determination, and after the individual IACs have been validated as compliant, non-compliant, or not applicable, a residual risk analysis (an analysis that determines risk due to partial or unsatisfactory implementation of assigned IACs) should be conducted. In order to determine the likelihood of a future adverse event, threats to a system must be analyzed in conjunction with potential vulnerabilities, along with the IACs that are in place for the system as well as the urgency of completing corrective action.

Two indicator codes aid in this analysis:

- Impact Codes
- Severity Categories

4.4.2.9.1 Impact Codes

Impact Codes are assigned to IACs at the time of authoring and maintained by the DoD DIACAP Technical Advisory Group (TAG). They indicate the TAG's assessment of the magnitude of network-wide consequences of a failed IAC and are used to assess community risk. Impact codes are expressed as High, Medium, and Low, where High is the indicator of greatest impact or urgency. In conjunction with the severity category, it also indicates the urgency with which corrective action should be taken. Within a severity category, non-compliant IACs should be prioritized for correction or remediation according to their impact codes.

Impact codes are listed on the IACs detail pages. A complete list can be accessed from within the IACs section of the DIACAP Knowledge Service.

4.4.2.9.2 Severity Categories

Severity categories in most cases are assigned by DISA for a system weakness or shortcoming. In those instances where severity is not already assigned, the CA or a designated representative, as part of a certification analysis, is required to indicate the risk level associated with the security weakness and the urgency with which the corrective action must be completed. Severity categories are expressed as CAT I, CAT II, and CAT III. Severity categories are assigned after considering all possible mitigation measures that have been implemented within system design and architecture limitations for the DoD IS in question. For instance, what may be a CAT I weakness in a component part of a system (e.g., a workstation or server) may be offset or mitigated by other protections within hosting enclaves so that the overall risk to the system is reduced to a CAT II.

4.4.2.10 Accreditation Decision

An accreditation decision is issued by the DON Service DAA, and is communicated via the accreditation statement, DIACAP Scorecard, IT Security POA&M, and any additional information that may be required. Documentation (e.g., artifacts, actual validation results) supporting an accreditation decision will be provided in electronic form if requested by DAAs of interconnecting systems. See Enclosure (13) for accreditation decision letter example.

The accreditation decision always applies to a specifically identified site or system and is based on a balance of mission or business need, protection of personal privacy, protection of the information being processed, and protection of the information environment, and thus, by extension, protection of other missions or business functions reliant upon the shared information environment. The accreditation decision is expressed as:

- Authorization to Operate (ATO)
- Interim Authorization to Operate (IATO)
- Interim Authorization to Test (IATT)
- Denial of Authorization to Operate (DATO)

Absent an accreditation decision, a system is considered Unaccredited.

The formulation of an accreditation decision is supported by the DIACAP package, and always requires a certification determination. If the C&A package evaluation is abbreviated due to mission urgency, the accreditation decision cannot exceed an IATO. If operation will be required beyond the time period of an IATO, a complete C&A package evaluation should be initiated immediately.

When there is compelling operational necessity, sites and systems may be allowed to operate despite IT security weaknesses that cannot be corrected or adequately mitigated within prescribed timeframes due to technology limitations or, in rare cases, prohibitive costs. Such instances must be fully justified, approved, and documented. The IT Security POA&M is used to document DAA-accepted non-compliant IACs and baseline IACs that are not applicable; however, the acceptance can only be indicated by the DAA. Unless specifically accepted, all IT Security POA&M items must continue to be evaluated for corrective actions and closure.

4.4.2.10.1 ATO

Authorization granted by a DAA for a site or system to process, store, or transmit information. An ATO indicates that a site or system has adequately implemented all assigned IACs to the point where residual risk is acceptable to the DAA. ATOs may be issued for up to 3 years.

Conditions: The ATO accreditation decision must specify an Authorization Termination Date (ATD) that is within three years of the authorization date.

A system with an unmitigated CAT I weakness may not be granted an ATO. A system can operate with a CAT I weakness only when it is critical to military operations as determined by

affected military commanders and if failure to deploy or allow continued operation for deployed systems will preclude mission accomplishment. Reference (c) provides further guidance for issuance of ATOs.

A system with an unmitigated CAT II weakness can be granted an ATO only when there is clear evidence that the CAT II weakness can be corrected or satisfactorily mitigated within 180 days of the accreditation decision.

An ATO can be granted with CAT III weaknesses. The DAA will determine if these weaknesses will be corrected or the risk accepted. CAT III weaknesses accepted by the DAA will appear on the IT Security POA&M with the "Resources Required," "Scheduled Completion Date," "Milestones with Completion Dates," and "Milestone Changes" columns marked "NA," and with the "Status" column marked "Risk Accepted by DAA." Only the DAA can annotate the "Status" column as "Risk Accepted by DAA"; until the risk has been accepted, the SO must continue to evaluate for corrective actions.

4.4.2.10.2 IATO

A temporary authorization to operate a site or system under the conditions or constraints enumerated in the accreditation decision.

An IATO accreditation decision is intended to manage IA security weaknesses while allowing site or system operation. It is not intended to be a device for signaling an evolutionary acquisition. A version of a system acquired in one of a planned series of acquisition increments or development spirals should be granted an ATO, even if additional or enhanced capabilities and services are planned for future increments or spirals.

Conditions: The IATO accreditation decision must specify an authorization termination date (ATD) that is within 180 days of the authorization date. A DAA may not grant consecutive IATOs totaling more than 360 days. A request for IATO must be accompanied by an IT Security POA&M. Corrective actions specified in the IT Security POA&M must be achievable within the authorization period and must be resourced accordingly.

If CAT II weaknesses have not been corrected or satisfactorily mitigated after system operation under IATOs for a total of 360 days, the DAA will normally issue a DATO that will remain in effect until all corrective actions identified in the IT Security POA&M are implemented satisfactorily and the DAA is able to grant an ATO. Reference (c) provides further guidance for issuance of IATOs beyond the 360 day time frame.

4.4.2.10.3 IATT

A temporary authorization to test a site or system in a specified operational information environment or with live data for a specified time period within the timeframe and under the conditions or constraints enumerated in the accreditation decision. Operation of a system under an IATT is for testing purposes only (i.e., the system will not be used for operational purposes during the IATT period).

Authorization is based on an assessment of impact to the information environment, or in the case of live data, an assessment of mission impact. In many cases, not all IACs need to be

satisfied for testing. In concert with the PM/SM, the DAA will determine what IACs must be satisfied for a specific testing event. The IATT accreditation decision establishes the agreed upon test duration and any special conditions or constraints, to include notification thresholds and addressees.

Conditions: The IATT accreditation decision is a special case for authorizing testing in an operational information environment or with live data for a specified time period. IATTs should be granted only when operational environment/live data is required to complete specific test objectives (e.g., replicating certain operating conditions in the test environment is impractical). All applicable IACs should be tested and appropriately addressed prior to testing in an operational environment or with live data except for those which can only be tested in an operational environment. In consultation with the PM or SM, the DAA will determine which IACs can only be tested in an operational environment. An IATT may not be used to avoid ATO or IATO validation activity and certification determination requirements for authorizing a system to operate.

4.4.2.10.4 DATO

A DATO will be issued if the DAA determines that a site or system should not operate because the IA design is inadequate, assigned IACs are not adequately implemented, or other security issues are revealed through certification. If the system is already operational, the DAA will issue a DATO directing the PM/SM/IAM to halt operation of the system immediately and may require the system to be de-installed from the network.

A DATO will also be issued if the PM has identified that the system has reached its end of life. In these cases, the DATO will be issued based upon the de-installation POA&M provided by the PM.

5.0 ROLES AND RESPONSIBILITIES

Central to the C&A process is a clear understanding of the roles and responsibilities of IT SO, 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 the DON IT infrastructure.

Within the DON, there are many significant roles in contributing to the secure development and operation of information technology systems. This handbook allows bureaus and officers of the DON to build 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, operations, maintenance, and disposal.

See Enclosure (1) Reference (ff) for further details.

5.1 DEPARTMENT OF THE NAVY CHIEF INFORMATION OFFICER (DON CIO)

As the senior IM/IT officer in the DON, the DON CIO is responsible for carrying out the Secretary of the Navy IA responsibilities assigned by the Federal Information Security Management Act (FISMA) of 2002 to the Head of each Federal Agency. Accordingly, the DON CIO shall ensure DON compliance with the IA requirements of FISMA, Enclosure (1) References (b), (c), (e), and related IA policies, procedures, standards and guidelines.

Per the 8510.01, the DON CIO shall:

- Appoint a DON Senior Information Assurance Officer (SIAO) in accordance with Enclosure (1), Reference (c), to direct and coordinate the DON IA Program that is consistent with the strategy and direction of the DoD IA Program.
- Ensure that the implementation and validation of IACs through the DIACAP is incorporated as an element of DON ISs life cycle management processes.
- Ensure that the DIACAP status of any DON IS is visible to the DoD CIO/SIAO and Principal Accrediting Authority.
- Ensure collaboration and cooperation between the DON IA Program and the PAA, and DAA structure.
- Ensure that a program or system manager is identified for each DON ISs.

5.2 DON Senior Information Assurance Officer (SIAO)

5.2.1 SIAO Definition

The DON SIAO is under the authority and direction of the DON CIO, and is responsible for the sustained IA posture of the Department. The DON SIAO ensures that IA and network security status within the DON are maintained and managed, and that status is subsequently reported to the DON CIO.

5.2.2 SIAO Accountability

The SIAO reports to the DON CIO and is designated in writing.

5.2.3 SIAO Responsibilities

In addition to responsibilities identified in reference (c), the DON SIAO is responsible for:

- Ensure that the DON IM/IT enterprise complies with requirements of applicable DON, DoD, and Federal policies and mandates such as the Clinger-Cohen Act (Title 40), USC Title 10, FISMA, DoDI 8500.1 and DoDI 8500.2. The SIAO shall establish a reporting relationship and improve alignment between the Navy and Marine Corps DAAs; facilitate a consistent application of Information Management, IT and IA policies, processes, responsibilities, and procedures consistently across the Department; ensure lines of communication to the operational chain of reporting between Service level DAAs and the DON SIAO; establish and enforce the C&A process within the DON IA program; and ensure DON level participation in the DoD DIACAP TAG.
- Establish an enterprise IA related posture in a risk-shared environment that allows for mitigation through the:
  - Integration of people, technology and operations.
  - Layering of IA solutions within and among IT assets.
  - Selection of IA solutions based on their related level of robustness.
- Coordinate risk management across the DON by ensuring that service DAAs balance threat against system/data criticality to identify and implement practical solutions.
- Ensure that IA is incorporated as an element of DON acquisition life-cycle management processes. Participate in updates to, and reviews of, DON acquisition guidance, such as the SECNAV 5000 series documents.
- Ensure that PII is treated as sensitive information.
- Ensure that DON CIO is kept informed of significant items (e.g., major mission degradation, major privacy concerns, shared lessons learned, and IA strategies) across the Enterprise.
- Ensure that consistent skill sets and the best use of resources to support a well-managed and competent IM and IT workforce across the DON in accordance with DoD and DON requirements.
- Encourage a robust program within the DON for vulnerability assessments and penetration testing, including effective use of red team exercises. Encourage sharing of lessons learned and best practices across the Navy and Marine Corps.
- Ensure that consistent application of waiver request standards and processing across DON networks.
- Coordinate efforts to achieve and maintain the DON in the GREEN status of the President's Management Agenda (at least 90 percent compliance) with FISMA

requirements. This effort would include identification and corrective action (including possible termination) for any application, system, or network that is not properly certified and accredited.

- Ensure that proper reporting under FISMA.
- Coordinate with the DON Component DAAs for implementation of joint or defense-wide programs.

All IT systems must register in the DoD Information Technology Portfolio Repository-Department of the Navy (DITPR-DON). Since some IT systems do not need to be reported under FISMA, the SIAO shall ensure functionality within DITPR-DON, which allows DON users to capture the security status of all DON IT assets while ensuring that proper FISMA reporting is maintained.

The DON SIAO is responsible for the development and execution of a formal certification process per applicable DoD instructions. The DON SIAO shall:

- Review all new Federal IT security requirements, NIST documentation, DoD Instructions and DON policies and procedures to correctly interpret them for their impact and consistency.
- Ensure that DON Deputy CIO (Navy) and DON Deputy CIO (Marine Corps) perform security verification reviews of IT systems per requirements under FISMA.
- Review reports prior to submission to the Office of the Secretary of Defense (OSD), the Office of Management and Budget (OMB), and the Government Accountability Office (GAO) as required under FISMA.
- Receive C&A data and results from the Navy Operational DAA (ODAA)/Marine Corps Enterprise Network (MCEN) DAA and document risk trends for the Navy and Marine Corps C&A process respectively.

5.3 Chief of Naval Operations (CNO) and the Commandant of the Marine Corps (CMC)

The CNO and the CMC are responsible for developing and implementing IA programs, procedures and controls, ensuring that IA is incorporated throughout the system development life cycle, appointing Designated Accrediting Authorities (DAAs), providing enterprise-wide vulnerability mitigation solutions, and providing incident reporting and response capability.

5.4 DON Deputy CIOs

The Deputy Chief of Naval Operations for Communication Networks (DCNO N6) serves as the DON Deputy CIO (Navy). The Director for C4, Headquarters Marine Corps (HQMC) serves as the DON Deputy CIO (Marine Corps). In carrying out their responsibilities as DON Deputy CIO, they report directly to the DON CIO and perform such duties and responsibilities as assigned by the DON CIO. DON Deputy CIO (Navy) and DON Deputy CIO (Marine Corps) are responsible for implementing and enforcing all relevant laws, policies, regulations, and procedures, including the strategies and policies promulgated by the DON CIO.

5.5 Designated Accrediting Authority (DAA)

5.5.1 Introduction

Accreditation is the formal declaration by the DAA that an IS is approved to operate using a prescribed set of safeguards at an acceptable level of risk.

The Navy has one operational DAA, multiple developmental DAAs at acquisition commands, and deployed DAAs described in subsequent paragraphs. The Marine Corps has one Marine Corps Enterprise Network DAA, developmental DAAs, and deployed DAAs, also described below.

5.5.2 DAA Definition

The DAA is a senior management official or executive with the authority to formally authorize the operation of an IT system at an acceptable level of risk. The DAA supports and enforces IA practices and principles by ensuring compliance with applicable IAC requirements throughout the IT system life cycle.

5.5.3 DAA Security Investigation, Position Designation, and Clearance Requirements

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 DoD8500.2 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 DoDI 8500.1 and Chairman Joint chiefs of Staff Manual (CJCSM) 6510.01. Exceptions to this policy may be made by prior coordination with and authorization from DON Deputy CIO (Navy) or 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 a developmental DAA residing at Marine Corps Systems Command (MARCORSYSCOM) and Marine Corps Tactical Systems Support Activity (MCTSSA). The Marine Corps also recognizes the role of deployed DAAs.

5.5.4 DAA Responsibilities

The DAA is responsible for ensuring that the DON C&A process is implemented. The DAA represents the interests of mission need, considers the operating environment, evaluates the impact to budget requirements and defines the acceptable level of risk to manage. Each DAA, in addition to satisfying all responsibilities of an Authorized User, shall:

- Satisfy all responsibilities and training outlined in DoD 8570.01-M, DoDD8500.1, DoDI 8500.2 and CJCSM 6510.01.

- Execute appropriate requirements for acquisition management listed in SECNAVINST 5239.3A.

While performing the role of Developmental DAA (DDAA) in the acquisition community (e.g., for a SYSCOM, developmental activity, Centrally Managed Program (CMP), or Program Of Record (POR)), the DDAA ensures that planned IACs for systems that will connect to operational networks are consistent with IACs required by the USN ODAA or MCEN DAA.

For SCI-specific responsibilities, refer to DCID 6/3 paragraph 2.B.5 and Joint DoD Intelligence ISs (DoDIIS) Cryptologic SCI ISs Security Standards (JDCSISSS) paragraph 1.5.3.

5.5.5 Operational DAA/MCEN DAA

The Navy's Operational DAA (ODAA) and the Marine Corps' MCEN DAA are the officials responsible for issuing a written authorization to operate applications, systems, and networks. This authority to operate includes all operational non-SCI and non-NC2-ESI systems, stand alone systems, business applications or services procured under CMPs/POR and non-CMPs/POR, major applications, and local, base, or wide area networks, including those used in support of exercises.

Authorization to operate is based upon two factors:

- The CA's comprehensive evaluation of the technical and non-technical security features of an IT system or network.
- The ODAA's/MCEN DAA's acceptance of residual risks and mitigation strategies to maintain an acceptable level of risk to operational (production) Naval networks.

The ODAA/MCEN DAA also approves all requests to connect any system or network to any operational enterprise network (e.g., Defense Research and Engineering Network (DREN), NIPRNET) regardless of the duration. Operational risk is balanced with mission need and the cost of securing the system or reducing the risk.

Prior to transition to, or initial use on, Naval enterprise networks, CMP/POR systems or locally-acquired IT assets will be approved for transition and accredited by the ODAA or MCEN DAA.

The ODAA reports to the DCNO N6. The MCEN DAA reports to the Director, HQMC C4I/CIO.

5.5.6 Deployed DAA

The senior commander, commanding officer (CO) or officer-in-charge (OIC) 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 is not to be used to circumvent normal configuration control processes, and should only be used in mission essential operational circumstances. Deployed DAAs notify the Navy ODAA/MCEN DAA via message or e-mail of all changes made to the security posture of the application, systems, or network as part of the transition of authority to the Navy ODAA/MCEN DAA once the ship, unit, or command returns to port or garrison. The Deployed DAA,

depending upon the service, reports to the ODAA or MCEN DAA concerning issues affecting the network/systems' IA posture.

5.5.7 Developmental DAA (DDAA)

The DDAA is the official responsible for ensuring completion of the DAA function for applications or systems during acquisition, development, Test and Evaluation (T&E) and risk mitigation prior to use or testing within the operational Naval enterprise.

When a system is ready for connection to an operational network for testing or use, the DAA role is shared between the DDAA and the ODAA/MCEN DAA. The DDAA ensures that IACs are implemented, tested and validated in a non-operational environment. Within the Navy, the ODAA issues an Interim Authorization to Test (IATT) to accept the risk of testing performed in an operational environment. Within the Marine Corps, this responsibility falls to the DDAA. DAA responsibilities fully transition to the Navy ODAA when an accreditation request is made for operation in the operational environment. Once a Marine Corps system under the DAA's cognizance reaches Milestone C of the acquisition cycle, the MCEN DAA will issue an accreditation decision allowing use within the operational environment. DDAA responsibilities for the system do not end until a successful IAC validation and subsequent risk assessment and certification are completed and a proper system handoff to the ODAA is accomplished.

The Marine Corps DDAA is responsible for C&A of IS (but not network) development prior to Milestone C of the acquisition process. Once a Marine Corps IS satisfies the requirement and is ready for deployment on an operational network, the Certifying Authority's Representative (CAR) assembles the accreditation package and submits it to the MCEN DAA for approval, and DAA responsibilities transition fully to the MCEN DAA.

5.5.8 Multiple Accreditors

Often, different components of a system fall under separate jurisdictions. The responsible authorities for those jurisdictions must collectively accredit the system. Generally, systems in these environments are divided into two types:

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

Written agreements are required when ISs interconnect. For example, connections between the Navy and the Marine Corps, or with other Services, or agencies, or with government contractors, would require an agreement before connecting the systems. 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 DAAs' 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, CAs, and other key security personnel of all participating organizations must be clearly defined and documented in the appropriate accreditation documentation.

5.6 Certifying Authority (CA)

5.6.1 Introduction

Certification is the comprehensive evaluation of the technical and non-technical security features of an IS and other safeguards to establish the extent to which a particular design and implementation meets a set of specified security requirements. The CA (and the Validator) provides the technical expertise to conduct this evaluation. At the completion of the certification effort, the CA determines the level of residual risk and recommends to the DAA whether or not to accredit the system based on their evaluation of the documented residual risk.

5.6.2 CA Definition

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 (IACs) stated in DoDI 8500.2 and other applicable DoD and DON requirements. The CA issues a recommendation to the DAA that includes an assessment of risk of operating the applications and/or systems. The accreditation recommendation is based on an evaluation of the threats imposed by the intended operating environment, vulnerabilities of the system, and mitigating actions applied to the vulnerabilities. The CA recommends appropriate restrictions or conditions for the consideration of the DAA in determining whether further risk management is necessary or accreditation should be issued.

5.6.3 CA Security Investigation, Position Designation, and Clearance Requirements

The CA is required to have an adjudicated security clearance commensurate with the level of access required, based on the Position Sensitivity Level and IT designation of the position commensurate with all IS under the CA's purview. All CAs must be U.S. Citizens.

5.6.4 Certifying Authority (CA) Responsibilities

The CA is responsible for making a technical evaluation of a system's 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 and accreditation recommendation to the DAA for consideration in making an accreditation decision.

The duties of the CA include:

- Evaluating the DIACAP Implementation Plan for soundness and thoroughness prior to signing the system's initial C&A documentation along with the DAA, PM and UR to indicate agreement with the system's architecture, security features and C&A plan.
- 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 the vendors who develop, host, or are otherwise involved with the DON systems are subject to the same or higher standards applied by the DON.

- Reporting the status of certification and providing a recommendation to the DAA whether or not to accredit a system based on documented residual risk.

CA performs functions described in CJCSM 6510.01 for collateral systems or Defense Intelligence Agency Manual (DIAM) 50-4 and JDCSISSS for intelligence community systems.

The organizations with CA responsibility for the Navy are:

- Nuclear Command and Control Extremely Sensitive Information (NC2-ESI) – USSTRATCOM J672.
- SCI (intelligence systems) – SSO Navy (ONI-53).
- Collateral (general service, GENSER) – SPAWARSYSCOM.

The Marine Corps CA is the Director, Information Assurance Division, Command, Control, Communications, and Computers Department. Marine Corps Systems Command (MARCORSYSCOM) is assigned as the CA representative for programs of record that are installed on an operational network. The Marine Corps CA has designated specific commanders as CA representatives for IS and networks under their control; these are the positions that were formerly known as local DAAs.

5.7 Validator

5.7.1 Introduction

The Validator provides an independent, third party validation of the correct implementation of applicable IACs, analyzes the test results, and provides the risk assessment to the CA for review.

5.7.2 Validator Definition

The Validator is responsible for conducting the validation procedures to confirm or establish by testing, evaluation, examination, investigation, or competent evidence that a DoD IS's assigned IACs are implemented correctly and are effective in their application.

The Validator performs the requisite preparatory steps and conditions, performs the actual validation steps, compares the actual results with the expected results, and analyzes the differences for impact and risk.

The Validator is responsible for providing the CA and the DAA with an accurate technical evaluation of the application, system, or network, documenting the security posture, capabilities and vulnerabilities against relevant IACs, and a drafting a statement of preliminary or residual security risks for system operation.

5.7.3 Validator Security Investigation, Position Designation, and Clearance Requirements

The Validator is required to have an adjudicated security clearance commensurate with the level of access required based on the Position Sensitivity Level and IT designation of the position commensurate with all IS under the Validator's purview. All Validators must be U.S. Citizens.

5.7.4 Validator Accountability

The Validator serves as a trusted agent of and reports to the CA while working with the PM, and UR.

5.7.5 Validator Responsibilities

The Validator is responsible for validating a system's compliance with all applicable IACs for an assigned DON system, including developing the appropriate test procedures if necessary, executing the test procedures and accurately documenting the results of security testing. The Validator updates the C&A validation report for the assigned system(s).

5.8 Program Manager (PM)

As part of the acquisition community, the PM designs, purchases, develops, and delivers systems to the Navy and Marine Corps. The DoD requires acquisition managers to address IA requirements for all weapon systems; Command, Control, Communications, Computer, Intelligence, Surveillance, and Reconnaissance (C4ISR) systems; and IT programs that depend on external information sources or provide information to other DoD systems per DoDD 5000.1.

5.8.1 PM Definition

The PM is the designated individual with responsibility for and authority to accomplish program objectives for development, production, and sustainment to meet the requirements defined in the Initial Capabilities Document (ICD), Capabilities Design Document (CDD), and Capabilities Production Document (CPD). The PM is therefore responsible for ensuring that those IA requirements in the capabilities documents are designed into the system and that all IA documents are completed per the C&A process. The PM provides for the entire life cycle management, including the maintenance of all security features and IAC compliance, of their systems and/or programs. For non-CMP/POR systems, the PM functions are performed by the command or organization official that has the requirement and has procured the IT asset. For these non-CMP/POR systems this role can also be referred to as System Owner (SO).

5.8.2 PM Responsibilities

The responsibilities of a PM include:

- Establish and maintain a formal system risk management program.
- Ensure that all systems complete the C&A process prior to implementation in an operational environment and are compliant with DoD, DON, and Marine Corps IA policies.
- Ensure that IA and C&A costs are included in their program budget and are recorded in the IT Security POA&M.
- Ensure that Information System Security Engineering is accomplished.
- Coordinate, manage, or provide oversight to ensure that system security requirements are identified, resourced, and implemented to provide an acceptable level of risk.

- Coordinate the determination of the MAC and CL of new or development systems.
- Identify and implement appropriate baseline IACs and appropriate policies with the coordination and approval of the CA and DAA.
- Plan and execute the C&A process according to DON C&A policy for programs that receive, process, store, display or transmit unclassified or classified information.
- Ensure that operational system configurations implement best security engineering practices, including maintaining configuration per approved and applicable federal and DoD standards and DoD STIGs.
- Coordinate with the CA and DAA to ensure that IA requirements are identified and built in to new software or system versions and/or releases.
- Ensure that Information Assurance Vulnerability Alerts (IAVAs) are implemented, managed, and reported in accordance with DoD, DON, and Marine Corps policies and procedures.
- Ensure that IT-related contracts specify that any IA or IA-enabled product complete a National Information Assurance Partnership (NIAP) evaluation prior to acquisition of those products.

5.8.3 PM Accountability

The PM is accountable to their organization, typically a program sponsor, PEO, or a SYSCOM Program Management Office, for overall cost, schedule, and performance reporting for the program. Additionally, there are many IA responsibilities that reside with the PM.

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 C&A package. The PM manages all aspects of the system throughout its life cycle, including tracking all installed instances of the system, collaborating with sites providing inherited IACs, collaborating with stakeholders throughout the C&A process, and maintaining the required level of security for the system.

5.8.4 System Owner (SO)

A System Owner (SO) is any entity who has the responsibility to develop and field an IS or attain an accreditation for an IS within the DON. For the purposes of DIACAP, the SO has the same role, responsibilities and requirements as a PM.

5.8.5 Information System Security Engineer (ISSE)

An individual that performs the Information Systems Security Engineering functions in support of capturing and refining information protection requirements and ensuring their integration into IT acquisition processes through purposeful security design or configuration.

The ISSE is responsible for the development and submission of the C&A package and all of its contexts for systems and programs in the developmental and acquisition process. The ISSE

works with system architects, engineers, and developers to ensure that IACs are designed and implemented into a system throughout the development process.

For sites, the ISSE is the individual who performs the Information Systems Security Engineering functions at that location. This could be a system administrator, IAO, IAM, Network Security Manager, or an engineer. The ISSE furnishes IA expertise and should be involved throughout the C&A process and the life cycle of the site/enclave/environment.

5.8.6 Information Assurance Manager (IAM)

The Information Assurance Manager (IAM) is the individual responsible to the PM (for systems) or Commanding Officer (for sites) for the proper execution of an effective IA program for their system or site. This individual is sometimes referred to as the Information Assurance Officer (IAO). However, the IAO is usually an individual responsible to the IAM for ensuring that the appropriate operational IA posture is maintained for a specific DoD IS or subset of the organization.

The IAM is the individual designated in writing by the commanding officer with the authority to execute the command IA program and ensure compliance with the service IA program requirements. The IAM is responsible to the local IA authority (Certifying Authority Representative (CAR) for Marine Corps) for ensuring the security of each IT system, and ensuring that it is approved, operated, and maintained throughout its life cycle per the DAA-approved C&A documentation. The IAM is responsible for assisting in creating and maintaining accreditation packages. When assigned to a POR system, the IAM is responsible to the PM for establishing, implementing, and maintaining the DoD IS IA program. The IAM's responsibilities include:

- Act as the primary IA technical advisor to the PM and maintain IA oversight of the system, monitoring for security, system or architecture changes that may affect the IA posture.
- Develop and maintain a command-level IA program in accordance with references (a) and (b) that identifies the IA architecture, requirements, objectives, policies, personnel, processes, and procedures to provide adequate security for all associated assets.
- Ensure that IA officers and privileged users are appointed in writing and provided oversight to ensure that they are following established IA policies and procedures.
- Ensure that all newly-appointed IAOs and privileged users meet all qualifications, including clearance and/or citizenship requirements.
- Ensure that information ownership responsibilities are established for each IS to include accountability, access approvals, and special handling requirements.
- Ensure that IA certification documentation is developed and maintained according to current C&A guidance by reviewing and endorsing such documentation and recommending action to the CA.
- Review and endorse all IS accreditation or certification support documentation packages.

- Maintain a repository for all C&A documentation and modifications pertaining to all IT assets within the IAM's purview.
- Ensure that security events are properly investigated and incidents are reported to the DAA. In addition, the IAM ensures that responses to IA-related alerts are coordinated and reported.
- Ensure that all sensitive and classified data is destroyed in accordance with DoD, DON, and Marine Corps policies.
- Maintain previously locally accredited IS's IA program.

5.8.7 Information Assurance Officer (IAO)

5.8.8 Introduction

The IAO is an individual accountable to an IAM for ensuring that the appropriate operational IA posture is maintained for a command, organization, site, system, or enclave.

The number of IAOs at a command is based on the structure and needs of the specific command or activity. Larger organizations and SYSCOMs may have multiple IAOs; however, in smaller organizations, the IAM may perform the roles of both IAM and IAO. When the magnitude of IA oversight requires it, multiple IAOs should be assigned. An IAO can be assigned for one or more systems/networks (e.g., deployed [major combat force] or garrison [base/post/camp] Network Operations Center (NOC); Regional Network Operations Security Center (RNOSC)). IAOs may also be assigned to a CMP/POR during the acquisition cycle to ensure that the proper IACs are being addressed during the design and development of applications or systems.

5.8.9 IAO Accountability

The IAO is appointed in writing by the commanding officer and is directly accountable to the IAM.

5.8.10 IAO Definition

The IAO is an individual accountable to an IAM for ensuring that the appropriate operational IA posture is maintained for a command, organization, site, system, or enclave.

5.8.11 IAO Responsibilities

The IAO responsibilities vary depending upon the size and mission of the command. An IAO could oversee a network (e.g., a Network Environment (NE) position titled Network Security Officer), be assigned to one system in a Computing Environment (CE) Position (e.g., POR, shipboard fire control for Tomahawk missile system), or be assigned to assist the IAM in executing administrative tasks (e.g., training, policy, tracking system and network accreditation for a large network or Enclave Environment (EE)). Each IAO, in addition to satisfying all responsibilities of an Authorized User, assists the IAM in meeting the duties and responsibilities of 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 to comply with DoD, DON, and Marine Corps IA policies and directives.
- Assist the IAM in performing the duties and responsibilities outlined above.
- Ensure that network, site, system, or application ISs are certified and accredited.
- Ensure that accreditation and/or certification support documentation packages for systems(s) for which the IAO is responsible are developed, maintained, and updated as required.
- Ensure that all IA-related processes are monitored and accessible only to properly-authorized individuals.
- Ensure that all users have the requisite security clearances and need-to-know and are aware of their responsibilities before granting them access to an IS.
- Ensure that all IT users and operators read, understand, and sign an appropriate Network Users Agreement (i.e., NIPRNET, SIPRNET, JWICS, etc.) prior to receiving access to IT resources.
- Ensure that IA and IA-enabled software, hardware, and firmware comply with the appropriate security configurations.
- Coordinate security procedures with the IAM and SSPs, 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 the Inspector General's office, ensure that the integrity of the investigation is maintained, prevent the loss or alteration of data potentially involved in the investigation, and keep the IAM and all other appropriate persons informed throughout the duration of the investigation.
- Ensure that the 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 continuity of operations plans (COOP) to ensure that confidentiality, integrity, availability, and recoverability of critical IS and data are achieved during and after an incident or disaster. Additionally, coordinate with the appropriate representatives to ensure that the COOP meets command objectives and is tested prior to system operation and annually thereafter. Contingency plans must also be 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, the SSPs, as required. The IAM, IAO and System Administrator (SA) positions should not be the same individual.

5.9 User Representatives (UR)

The UR is one of the stakeholders who represent the operational interests of the user community to ensure the IT system meets the user needs. The UR must review the DIACAP 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 IACs have been identified, assigned, and validated so that the system still meets the user community needs when all of the IACs are fully implemented. The UR will identify and document any IACs that interfere with the mission execution and work to resolve these issues. Unlike the other stakeholders, there is not one organization that provides a person to fill this function. For new/development systems, PMs must obtain a UR from an organization that can provide a volunteer. URs do not require a high level of IA knowledge because their function is to provide a balance between operational (functional) and security requirements to ensure that the resulting security features are not so restrictive that users develop work-around for them and/or that the system will be under-utilized due to the users finding it too difficult to use. URs should be briefed on their duties and expectations that they will provide a thorough and honest representation of the user community and that they should be available to participate as a stakeholder throughout the C&A process.

6.0 DON DIACAP

This section explains, in detail, the DON implementation of the DIACAP for taking a system or site through all the C&A activities from cradle to grave. The transition to this process was necessary due to changes in IT and the threat environment, changes in the way the DON acquires, operates, and uses information technology, and to comply with federal requirements and mandates. The DoD has defined the C&A process as a series of activities in a never-ending cycle illustrated in Figure 9. While the DIACAP offers a valuable strategic view, this handbook and accompanying Service unique guidance, expands this strategic view down to the detailed step-by-step tasks that need to be completed for DON IS so that an accreditation decision can be reached in a timely manner and the accreditation is maintained throughout the system's life cycle.

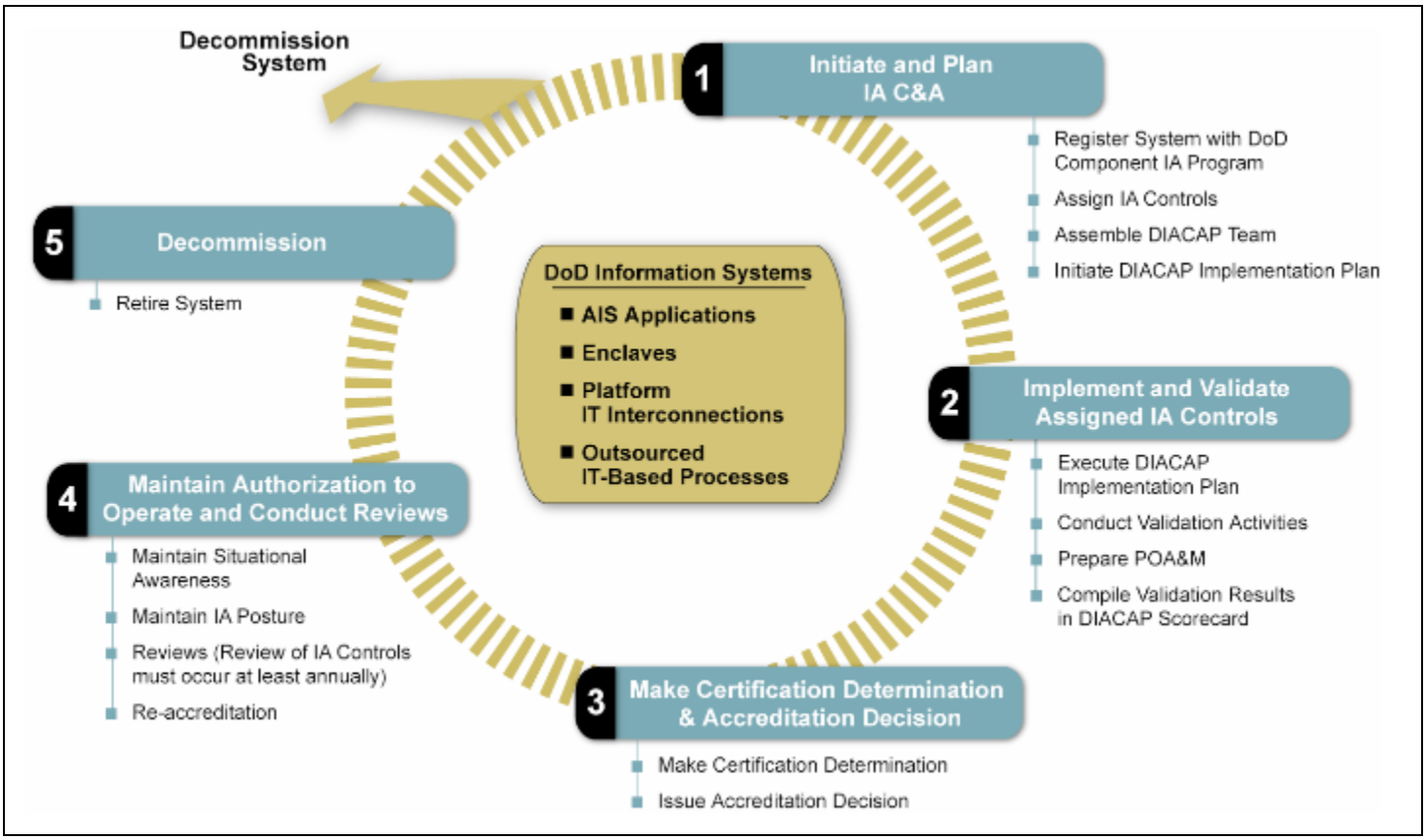


Figure 9. DoD DIACAP Cycle Overview

The methodology described herein will provide an efficient risk assessment of DON systems and networks in order to attain full accreditation and maintain it afterward. By properly verifying the correct implementation of the prescribed IACs, DON ISs should be able to be operated at an acceptable level of risk.

Most of the activity tasks are nearly identical for system and site accreditations; therefore, the term "system" will be applied generically to both systems and sites unless specifically differentiated. Additionally, ISSE is used to note the person performing the IS Security Engineering function which could be conducted by a designated security engineer, an IAO, IAM, system administrator, or somebody else. An ISSE may be used to perform IS Security Engineering tasks but this position may not be resourced or staffed as a separate entity. The term PM is used generically as a system program manager, SO, or any other person responsible for the system or site to attain an accreditation.

6.1 Overview

The DIACAP begins in Activity 1 by registering the IS seeking accreditation, gathering and refining the set of standardized IACs and their associated validation procedures, and assembling other documentation required to make an accurate risk assessment into a DIP. This set of documents will continue to be expanded, refined, and updated throughout the C&A process. Additionally, the DIACAP team is assembled and the DIP is submitted for review and concurrence. This team consists of the PM, Echelon II/MSC, CA, DAA, UR, and will be referred to generically as the stakeholders for the system undergoing C&A. For the Navy, review activities are accomplished via the collaborative process.

During Activity 2, the DIP is executed, tests are conducted, test results are compiled and reviewed by the Validator, and other activities necessary to comply with required IACs are documented in an IT Security POA&M. The ISSE/PM assembles the complete C&A documentation, now known as a C&A package, and submits it for review by the UR and the Echelon II/MSC and subsequent forwarding to the CA. For the Navy, review activities are accomplished via the collaborative process.

In Activity 3, the CA and DAA review the C&A package and assess the level of residual risk. If the level of risk from the remaining vulnerabilities (non-compliant IACs) is acceptable, a certification determination is made by the CA, who provides a risk determination and recommendation for accreditation to the DAA. The DAA reviews the CA's recommendation and issues the accreditation decision by issuing an ATO, IATO, IATT or DATO.

In Activity 4, the system is installed, tested in its installed environment, and is then reviewed annually to ensure that the system remains in compliance with the IACs. If there is a significant change to the IS's security profile, a security incident occurs, or three years have elapsed since the last accreditation, the system cycles through the process for reaccreditation.

Activity 5 is at the end of the system's life cycle, when the system is decommissioned and removed from service. The appropriate information repositories are then updated with the status change of the system. The DAA issues the DATO.

These activity steps are summarized in Figure 10.

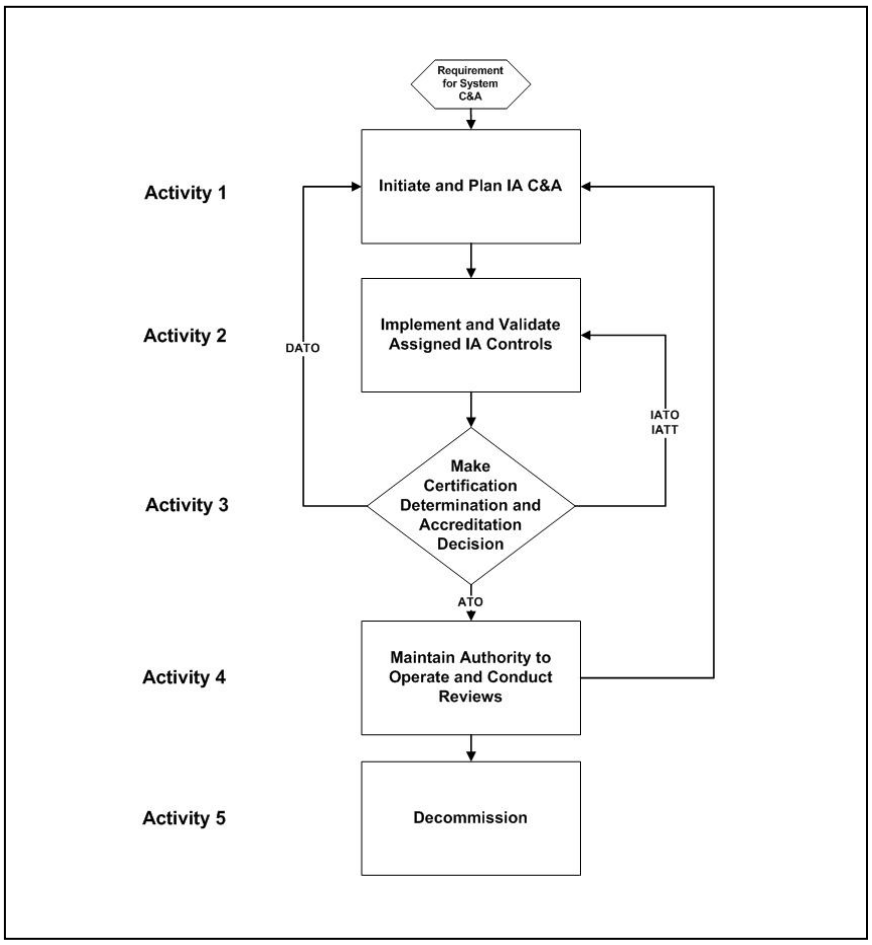


Figure 10. DIACAP Activities

The DON implementation of DIACAP described in this handbook is the outcome of a comprehensive process engineering effort where the above activities were thoroughly analyzed as they were decomposed into successive levels, providing increased detail with each level. The process flow was then subjected to several reviews at various levels, which included the Fleet and Program Offices, CA, and DAA, to ensure that it accurately reflected the required tasks at each level and that it could be supported at all levels. The remainder of this handbook provides the detailed explanation of the validated steps that resulted from this process engineering effort.

6.2 Activity 1 - Initiate and Plan IA C&A

In this section we will explain what is necessary to accomplish the following tasks:

- Initiate the DIACAP Package.
- Assign IACs and other requirements.
- Complete and submit DIP.
- Gain DIP Concurrence.

To initiate the C&A process and plan the future C&A activities and tasks, the PM/SO or ISSE must begin gathering data on the system that will be certified and accredited, and must put together the plan that will be used to achieve accreditation. Using the data, the PM/SO or ISSE needs to register the system within DITPR-DON or DADMS, following MILDEP guidance and service-unique direction. All relevant IACs, along with how the IACs will be validated, are identified and organized into a DIP for submission to the C&A chain for concurrence.

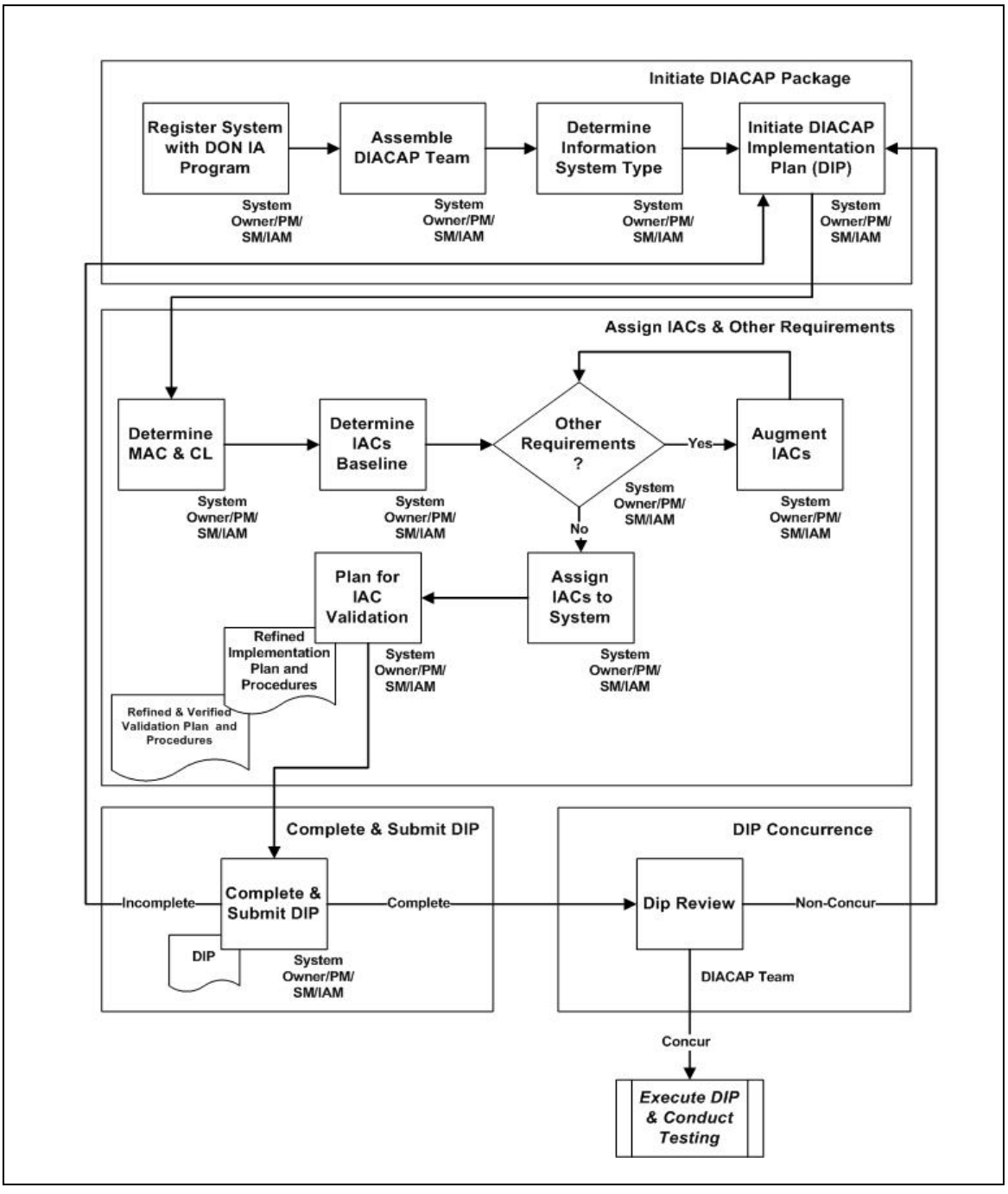


Figure 11. Activity 1 – Initiate and Plan IA C&A

6.2.1 Initiate DIACAP Package

6.2.1.1.1 System Registration

The DON Application and Database Management System (DADMS) and DITPR-DON are the DON authoritative data sources for the registration and management of all DON IT (to include National Security Systems (NSS)) assets. Applications and networks are registered in DADMS and managed internally within the DON for IS registration, Enterprise Architecture, and IA assessments. Systems are registered in DITPR-DON not only for internal DON asset management, but more specifically for external reporting to DoD and to Congress, to include FISMA reporting. The ISSE is responsible for ensuring that all systems, applications and networks are registered in DITPR-DON and DADMS. The ISSE may coordinate this action with a Program Manager or Technical Manager following MILDEP-specific guidance and service-unique direction. An approved, government-sponsored DADMS/DITPR-DON account is required for the registration of all systems, applications, and networks. The web site to obtain an account and access DADMS and DITPR-DON is https://www.dadms.navy.mil.

During system registration, the ISSE or person making the entry must provide specific information required to complete all mandatory DITPR-DON data fields, as well as all conditional data fields that may pertain to an individual system. Much of this information, including the DITPR-DON identification number, must be entered on the SIP. DADMS registration entails completing the DADMS Central Design Activity (CDA) Questionnaire with the required information unique to the application. Once the DADMS CDA Questionnaire has been submitted, it will be reviewed by the assigned Function Area Manager (FAM). FAM approval must be obtained in order for the application to be eligible for use by the Navy or Marine Corps. For network registration, all basic information, including devices, servers, and applications, must be provided. The DADMS identification number must be entered on the SIP for both applications and networks.

6.2.1.1.2 Register the System with the DON IA Program

In order to meet the DIACAP requirement to register with a component specific IA database, the system needs to be registered with the DON designated IA tracking program/database for its specific service. Presently, the Navy should register in IATS at https://iats.spawar.navy.mil/, and Xacta for the Marine Corps at https://hqtelosweb.hqmc.usmc.mil/. Registration with the IA program identifies the system and provides the Echelon II/MSC, CA, and DAA with visibility of the system as it goes through the C&A process. For the Navy, registration is accomplished by creation of an IATS entry and completing a preliminary SIP. For the Marine Corps, all steps accomplished are via Xacta.

6.2.1.1.3 Creating a Preliminary SIP

The ISSE will enter as much of the program information as available into the SIP template to create the preliminary SIP. (See Enclosure (5) for an example SIP template and a description of the data elements of the SIP.) The most current version of the SIP and all the DIACAP templates can be found at https://www.fleetforces.navy.mil/netwarcom/navycanda/default.aspx by searching the site for "SIP" for the Navy or https://hqtelosweb.hqmc.usmc.mil/ for the Marine Corps. Once created, the SIP becomes a living document that will be continually updated throughout the life cycle of the program. This SIP provides the basic description or metadata about the system being certified.

6.2.1.2 Assemble the DIACAP Team

This step formally identifies and records the stakeholders of the system's C&A process. This team consists of the PM, Echelon II/MSC, CA, DAA, and UR.

The Echelon II/MSC point of contact would usually be the responsible IA official in the Echelon II/MSC within the chain of command of the PM/SO. The UR is identified by the PM/SO and should function as an independent representative of the user community to provide input on the impact of the IACs to the user community. Besides formally designating the UR, the PM/SO should ensure that they are aware both of their duties and responsibilities and of the expectation that they will be involved with the C&A process at various points. The ISSE obtains both a CA and DAA staff POC for coordinating any questions or issues throughout the C&A process. Collaborating with the same person helps achieve consistency across all issues and provides familiarity with the C&A package from the beginning.

The ISSE documents the DIACAP team on the SIP and forwards a copy to each of them. Each member of the team then acknowledges receiving the SIP, and the CA and DAA file the SIP as reference that a C&A package is in progress.

6.2.1.3 Determine IS Type

The PM/SO and ISSE must determine whether the system will be certified and accredited as a system or as a site. Before proceeding, the PM/SO and ISSE must also determine the MAC and CL applicable to their system because the IACs that will be assigned are directly dependent on the MAC and CL of the system.

6.2.1.3.1 Determine if the system will accredited as a System or a Site

Using the details for making the MAC and CL determination provided in the following paragraphs, the ISSE must determine if the IS will be accredited as a system or as a site. The default accreditation is as a system unless the PM/SO/ISSE specifies that it is a site. If a determination is made for a site accreditation, the Site Manager is responsible for determining MAC and CL. Remember that a site is an aggregation of individual systems. To summarize, system accreditations include:

- System
- Type
- Platform IT Interconnections
- Outsourced IT Processes

Site accreditations include:

- Site
- Network
- Enclave

Once the determination is made, the PM/SO and ISSE will initiate the DIP as described in section 6.2.1.4.

6.2.1.3.2 Determine the MAC and CL for the System

Descriptions of MAC and CL are provided in section 4.3.2 above. Using these definitions and descriptions, the ISSE, with PM concurrence, assigns the appropriate MAC and CL. This is recorded on the SIP, and will drive the baseline IACs for the system. To recap, the choices are contained in the following table:

MAC	Description
I	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. MAC I systems require the most stringent protection measures.
II	Systems handling information that is important to the support of deployed and contingency forces. The consequences of loss of integrity are unacceptable. Loss of availability is difficult to deal with and can only be tolerated for a short time. MAC II systems require additional safeguards beyond best practices to ensure assurance.
III	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 consequences of loss of integrity or availability can be tolerated or overcome without significant impacts on mission effectiveness or operational readiness. MAC III systems require protective measures, techniques or procedures generally commensurate with commercial best practices.
CL	**Description**
Classified	Systems that contain information specifically authorized under criteria established by Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy. This includes information designated or classified as Confidential, Secret, and Top Secret.
Sensitive	Systems containing information for which the loss, misuse, or unauthorized access to or modification of, could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under

MAC	Description
	Section 552a of title 5, United States Code, "The Privacy Act", but which has not been specifically authorized under criteria established by Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy. Examples of sensitive information include, but are not limited to, information in DoD payroll, finance, logistics, and personnel management systems. Sensitive information sub-categories include, but are not limited to, the following: For Official Use Only (FOUO), Privacy Data, DoD Unclassified Controlled Nuclear Information (DoD UCNI), Unclassified Technical Data, Proprietary Information, Foreign Government Information, Department of State Sensitive But Unclassified (DoS SBU), and Drug Enforcement Administration (DEA) Sensitive Information.
Public	Official DoD information that has been reviewed and approved for public release by the information owner in accordance with DoD Directive 5230.9.

6.2.1.4 Initiate the DIP

The next step in the process is to produce the DIP. This entails considerable effort to gather, refine, and assemble the various components of the DIP. The initial standardized list of IACs is predetermined based on the MAC and CL that were determined in the previous step.
The following are the components of the DIP:

- C&A Plan
- IAC Implementation Plan
- Validation Plan & Procedures
- Previous C&A statements (if system is being reaccredited or is operating under interim authorization)
- DIP Concurrence Sheet

The components of the DIP are listed in Enclosure (5) of this handbook.

6.2.1.4.1 Draft System C&A Plan

The ISSE develops the DIP that specifies how the system/site will meet C&A requirements.
A major component of the DIP is the C&A Plan, which contains, at a minimum, the following elements:

- Mission Description
- Concept of Operations (CONOPS) Summary
- Operating and Computing Environment
- User Description and Clearances
- Security Roles
- Hardware List

- Software List
- Ports, Protocols and Services (PPS)
- System Architecture Diagram
- Accreditation Boundary
- External Interfaces and Data Flow
- Contingency Plan
- Threat Analysis
- Physical Security Measures/Facilities
- C&A Tasks and Milestones
- Life Cycle Management Plan
- Other information as required

Enclosure (6) provides examples and templates to assist the ISSE in drafting the C&A plan. Once completely filled in, these templates, documents, and forms make up the C&A Plan, providing some of the essential elements of information that enable the CA to make a certification determination and the DAA to make an accreditation decision. These elements will be continually updated with additional information and changes throughout the C&A process and the system's life cycle.

6.2.2 Assign IACs and Other Requirements

6.2.2.1 Determine the IACs Baseline

The MAC and CL values that have been determined are used to obtain the IAC baseline by filtering the complete set of IACs and their associated test procedures down to those that are required by the particular MAC and CL levels of the system.

6.2.2.1.1 Create list of standard IACs

The ISSE can download the IACs and their associated test procedures at https://www.fleetforces.navy.mil/netwarcom/navycanda/default.aspx. USMC commands use Xacta to perform this function. The IACs with their associated test procedures are downloaded in spreadsheet format and form the basis for the IAC Implementation Plan, the Validation Plan and Procedures, and the IT Security POA&M. The spreadsheets have macros and the ISSE may receive a dialog box asking if the macros should be enabled or not. Macros need to be enabled in order for the spreadsheet functions to work properly.

6.2.2.1.2 Create Initial IAC Implementation Plan and Validation Plan and Procedures

The ISSE downloads the IAC controls as directed by their Service DAA. If using the above link to download the IAC spreadsheet, the ISSE must choose one of the nine possible MAC/CL combinations named files to download. Each file contains the required IACs for that MAC/CL

combination. In the downloaded file, one tab is for the IAC Implementation Plan, the other is for the Validation Plan and Procedures.

The ISSE saves the spreadsheet containing the two worksheets that they have just downloaded as the Initial IAC Implementation Plan and the Initial Validation Plan and Procedures documents. These initial documents will continue to be tailored as the ISSE works toward the final versions of these documents.

6.2.2.2 Determine Any Other Requirements and Their Associated IACs

Based on system characteristics, this initial list is augmented, if necessary, by additional IACs and their associated test procedures required by other programs, laws, regulations, or service-unique requirements. The PM, program office, or program sponsor should provide some insight or guidance into these additional requirements. Some research by the ISSE will most likely be needed if some additional requirements such as HIPAA, NIST, DCID, etc., are to be met.

When there are additional requirements that apply to this system/site, the ISSE first identifies the new requirements, and then identifies all the IACs that correspond to these additional requirements. The ISSE then adds these additional requirements and associated IACs and test procedures to the initial set of IACs identified previously.

If there are no additional requirements, the ISSE completes the list of applicable IACs and test procedures.

6.2.2.3 Assign IACs to System

The ISSE now analyzes this complete list of IACs, documenting the justification for those IACs that are not applicable, and identifying the IACs that are either inherited or inheritable. These actions lead to a finalized list of applicable IACs, and the updating of both the Initial IAC Implementation Plan and the Initial Validation Plan and Procedures to ensure that they contain these changes.

6.2.2.3.1 Identify and Document Non-Applicable IACs

The ISSE must analyze this initial baseline list of IACs and determine which, if any, are not applicable, based on system characteristics or capabilities. If any IAC is determined not to be applicable, the ISSE documents the reason for this determination in the appropriate location in the Implementation Plan and the Validation Plan and Procedures.

6.2.2.3.2 Determine Inherited/Inheritable IACs

During the analysis of the IACs, the ISSE determines which IACs can be inherited from the system's target environment or are inheritable by other systems. The ISSE will document these inheritance relationships in the IAC Implementation Plan (see Enclosure (7)).

6.2.2.3.3 Finalize List of Applicable IACs

Once this analysis is complete, the ISSE ensures that both the IAC Implementation Plan and Validation Plan and Procedures have been updated and are in synch with each other (control for control). As a final check, these plans contain the final listing of IACs; all non-applicable IACs are identified with supporting justification documented, and the inheritability of IACs is recorded.

6.2.2.4 Plan for IAC Validation

With the updated initial IAC Implementation Plan and initial Validation Plan and Procedures, the ISSE can now work on fleshing out the details of how these IACs will be implemented and how they will be verified in their systems.

6.2.2.4.1 Refine the IAC Implementation Plan

The ISSE reviews the architecture of the system/site and the related system development documentation. Working with the system's architects, engineers, and/or developers, the ISSE develops guidance on how each IAC should be incorporated into the system architecture so that each device, configuration or feature will meet IA requirements. This guidance is part of the IAC Implementation Plan and should be recorded in the appropriate fields.

The ISSE determines who will be responsible for the implementation of each IAC, the implementation status, the resources required for their implementation, and the estimated completion date for each assigned IAC.

To complement this effort, the ISSE also identifies the applicable supporting implementation materials and artifacts. During the system's continued development, the ISSE will monitor and track the correct implementation of necessary actions per the implementation plan.

Once this more detailed implementation planning is completed, the ISSE updates or modifies the IAC Implementation Plan to support the target/planned architecture. Updates to this plan should be saved as a Refined IAC Implementation Plan, by version if necessary.

The goal during the development process is to properly incorporate all applicable IACs into the system as specified in the IAC Implementation Plan while the system is being developed. This ensures that the system architectural components are selected with adequate IAC compliance, and avoids having to retrofit security into the finished system. The ISSE continues to refine the IAC Implementation Plan as the system undergoes development so that system development and planned implementation of IACs are always in alignment.

6.2.2.4.2 Refine Validation Plan and Procedures

With the IAC Implementation Plan mapped to the target architecture, the ISSE can now refine the corresponding Validation Plan and Procedures. This process is started with a review of the IAC Implementation Plan and the C&A Plan.

The ISSE collects the associated applicable supporting materials and artifacts. The ISSE synchronizes the refined IAC Implementation Plan with the initial Validation Plan and Procedures, and ensures that there are validation steps and expected results for each identified IAC. Each Validation procedure must be reviewed for adequacy, thoroughness, and repeatability.

Proper test procedures are written in such a way that they are able to be executed by a person who did not develop them and still achieve the same expected results. This requires a level of detail that addresses each step to be taken in the validation procedure, precisely how it is to be executed, exactly what information is to be captured, and what the result is expected to be.

Once this analysis is completed, the ISSE coordinates with the DIACAP team to gain permission to modify and/or augment the initial Validation Plan and Procedures. This document is saved as an updated version as the Refined Validation Plan and Procedures.

The goal during this step is to ensure that test procedures contained within the Refined Validation Plan and Procedures adequately address all IACs. The ISSE continues to refine the Validation Plan and Procedures until it does.

6.2.2.4.3 Verify Validation Plan and Procedures

To the degree possible at this stage, the ISSE exercises the Refined Validation Plan and Procedures against the proposed system/site to verify that all applicable IACs have been addressed and that the validation procedures are adequate and repeatable. This means a comparison of the security requirements (IACs) and the system design document (Validation Plan & Procedures) will be accomplished prior to any task associated with the actual development, acquisition, or construction of the system.

For any identified weaknesses or unexpected results, the ISSE continues the refinement effort until the Validation Plan and Procedures are sufficiently comprehensive, reliable, and repeatable.

6.2.3 Complete and Submit the DIP

When all the IACs have been identified, the IAC Implementation Plan has been finalized (to this point), and the Validation Plan and Procedures has been completed, the ISSE will finalize the DIP for C&A stakeholder (i.e. the DIACAP Team) approval. The ISSE gathers the DIP components, makes any needed updates to both the DIP and SIP, drafts the DIP concurrence sheet to capture approval signatures for the DIP, and submits the DIP to the PM/SO for concurrence. Once the PM/SO concurs, it is then submitted to the DIACAP Team for review and approval.

6.2.3.1 Collect the DIP Components

The ISSE collects the DIP components consisting of the following:

- Any previous C&A Statements (normally for re-accreditation).
- The final IAC Implementation Plan.
- The final Validation Plan and Procedures.
- The C&A Plan collection of documents (see both paragraph 6.2.1.4.1 and Enclosure (6) for C&A Plan components).

6.2.3.2 Review the DIP

The ISSE conducts a final review of the DIP for completeness and accuracy. Any missing items must be added and any inaccuracies must also be corrected by returning to the preceding steps. The DIP must be as complete as possible before it can be submitted for concurrence and approval.

When the DIP is both accurate and complete, the ISSE creates the DIP concurrence sheet, and adds this sheet to the DIP.

For a system/site that is not yet operational, the ISSE submits both the DIP and SIP to the PM and the UR for their review. The PM should agree with the required resources necessary to comply, and the timeline should coincide with the acquisition timeline of the system. The UR should agree that the security features are viable and realistic in the environment that the system will be used.

A collaboration meeting between all the stakeholders will be scheduled to reach an agreement on key elements and the way forward. There may be instances where not all of the IACs will be in compliance or where resources are not available to complete necessary actions. This collaboration step ensures that all stakeholders are apprised of the situation and that they agree on the necessary actions to move forward in the development and accreditation process. This step is a necessary precursor to executing the Validation Plan and Procedures. After determining the way ahead, and agreeing to the necessary actions, the PM or IAM will eventually execute the DIP after it is approved.

6.2.3.3 Review and Concurrence by the Program Manager and User Representative

The UR reviews the SIP and DIP. If they do not concur, the package is returned to the ISSE to fix the identified areas. With proper liaison and collaboration, there should be no issue with the UR not concurring.

The PM reviews the SIP and DIP. If there are any issues, the package is returned to the ISSE to fix the identified areas. If regular updates have been provided to the PM/SO during the formulation of the DIP, the PM should be in full agreement after discussing the package with the other stakeholders.

After formal concurrence by both the UR and the PM/SO, each signs the DIP Concurrence Sheet in the appropriate place if conducting this manually. The SIP and DIP are then forwarded to the Echelon II/MSC for their review and concurrence.

6.2.4 DIP Review and Concurrence

The DIP is first reviewed by the Echelon II/MSC, followed by the CA and then the DAA. With previous collaboration, any potential issues should be known and should be worked out or agreement reached before they receive the package. If any problems or issues surface at this stage, they are documented by the party identifying them before returning the DIP to the PM/SO for resolution. When the Echelon II/MSC concurs, they sign their portion of the DIP Concurrence Sheet and forward the DIP to the CA. When the CA concurs, they sign their portion of the DIP Concurrence Sheet and forward the DIP to the appropriate DAA for their review and approval. Non-concurrence by the DAA sends the DIP back to the CA with their comments on the reasons for non-concurrence. When the DAA concurs, they sign their portion of the DIP Concurrence Sheet and return the DIP to the PM/SO with any comments for execution.

6.2.4.1 Echelon II/MSC Review the DIP

The Echelon II/MSC acknowledges receipt of the DIP and conducts a review of the DIP for supportability and sustainability. Echelon II/MSC updates the status of the system for FISMA reporting and reviews the Life Cycle Management Plan for the system. If they agree with the plan, they add a supportability and sustainability statement to the C&A package indicating IA life cycle management supportability responsibilities. With proper prior liaison between the PM and Echelon II/MSC, there should be no unknown issues that surface during this review.

The Echelon II/MSC documents their concurrence with the DIP by signing the DIP Concurrence Sheet, and forwards the DIP to the CA. If the Echelon II/MSC does not concur with the DIP or with the supportability and sustainability, they return the DIP with their comments to the PM for resolution; proper collaboration will prevent this from occurring.

6.2.4.2 CA Review the DIP

The CA acknowledges receipt of the DIP to the Echelon II/MSC and PM.

Packages are prioritized and tracked as they are received by the CA staff. A reviewer is assigned to review the DIP and make comments on the technical plans for IAC compliance. Ideally, this reviewer would be the same person that functioned as the POC for the PM, since they would already be familiar with the system, but due to workload and prioritization of packages within the CA's office, this may not always be the case. The CA reviewer analyzes the DIP to ensure that IA planning is sufficient to meet certification requirements. The reviewer confirms that the IACs are appropriate to the MAC and CL, the IAC Implementation Plan is sufficient to meet certification requirements, and the Validation Plan and Procedures are robust and developed with sufficient rigor and repeatability. The reviewer may also record helpful comments for the benefit of the PM/SO in managing and maintaining IA compliance.

If the CA reviewer identifies a problem with the plans, they should collaborate with the PM/SO to determine if there is a quick and reasonable solution to prevent the package from being held up. The reviewer records any comments, whether major or minor, to the DIP and forwards it to the CA for concurrence.

The CA reviews the package with the reviewer's comments and determines if he/she concurs with the DIP. If the CA does concur, the CA signs the DIP Concurrence Sheet and forwards the package to the DAA.

If the CA identifies any unresolved corrective actions that are required by the PM/SO, the CA returns the DIP to the PM/SO with comments that detail all required corrective actions. The Echelon II/MSC receives a copy of these comments for their information..

6.2.4.3 DAA Review the DIP

The DAA acknowledges the receipt of the DIP to the CA, Echelon II/MSC, and PM/SO. A staff reviewer is assigned to review the package. In much the same fashion as the CA review, this reviewer would ideally be the same person that functioned as the POC for the PM since they would already be familiar with the system, but due to workload and prioritization of packages within the DAA's office, this may not always be the case. The reviewer examines the package and the CA's comments for issues or concerns that may affect the operational environment or have a negative impact on other systems in the GIG environment. The reviewer attaches their comments to the package and sends it to the DAA for concurrence and signature.

If the DAA concurs with the reviewer's and CA's comments, they sign the DIP Concurrence Sheet and return the approved DIP with any comments to the PM/SO for execution.

If the DAA does not concur with the CA's comments/recommendations, they return the DIP to the CA with their comments detailing why they do not concur. The CA then tries to resolve the issue, which may require returning the package to the PM/SO for resolution.

With proper coordination and collaboration between the PM, Echelon II/MSC, CA, and DAA, all issues should be worked out in advance to avoid having a package returned for corrective action.

6.3 Activity 2 - Implement and Validate Assigned IACs

In this section we will explain what is necessary to accomplish the following tasks:

- Execute DIP and conduct testing.
- Compile the test results.
- Develop IT Security POA&M.
- Complete the C&A package.
- Echelon II/MSC Review for certification recommendation.

The workflow described in this activity depicts new system development. For existing systems, some portions of this activity may have already been accomplished, but are provided here for full understanding.

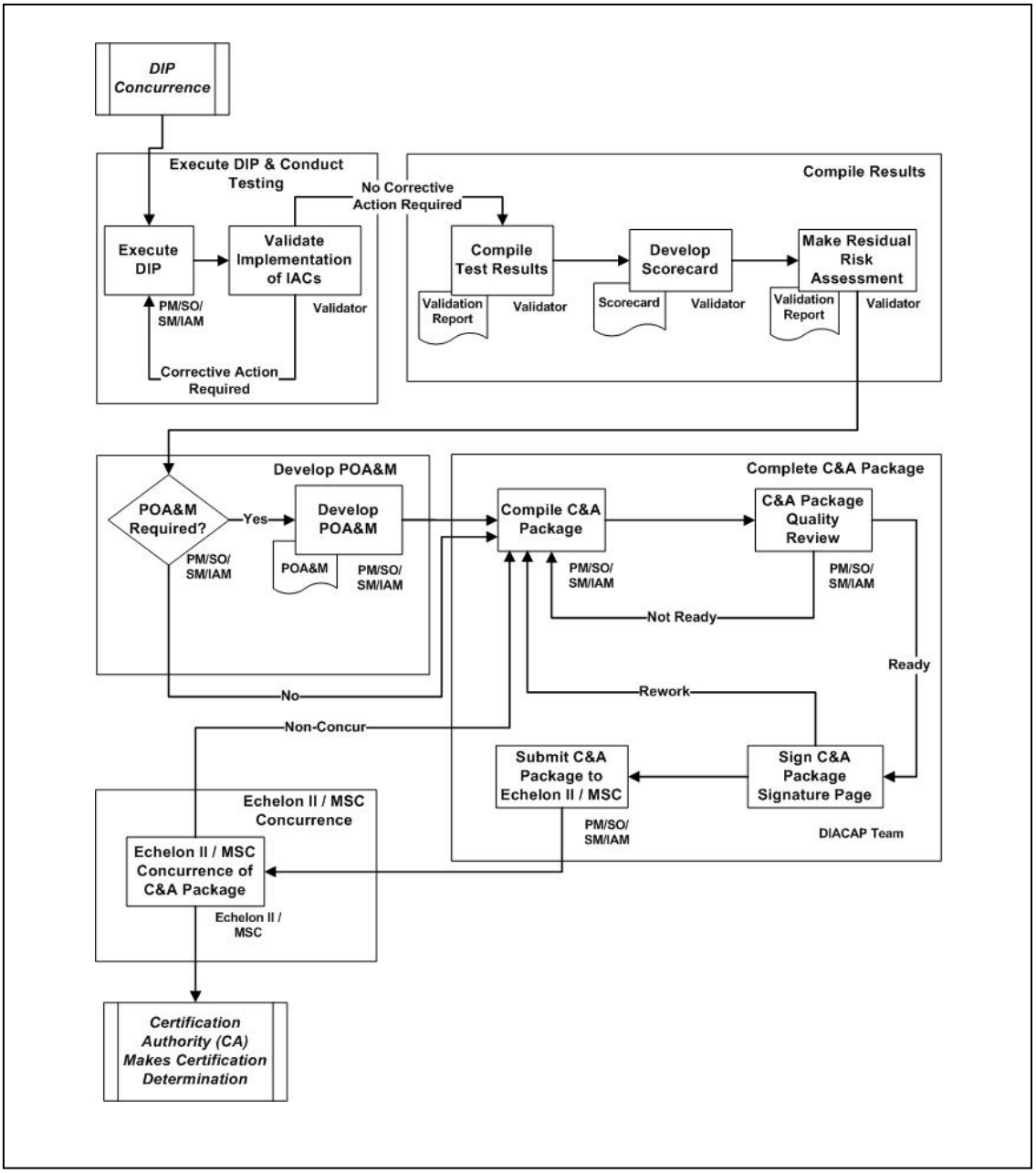


Figure 12. Activity 2 – Implement & Validate Assigned IACs

6.3.1 Execute DIP and Conduct Testing

For new systems development, this part of the process could be quite lengthy depending on the complexity and system acquisition timeline. The requirements delineated in the DIP to comply with the IACs are implemented and validated during this task.

6.3.1.1 Execute DIP

During system/site development, the PM/SO/ISSE executes the DIP to implement the required IACs and validate their implementation to ensure that they have been incorporated properly and are functioning correctly. Any identified discrepancy should be fixed, and the DIP is updated with all changes necessitated by evolving technology, threat environments, or unforeseen circumstances. When the IACs are completely implemented and ready to be tested, the ISSE or IAM complete any required preparations to support validation testing before notifying the CA that the system is ready for testing. The Validator is selected and the testing date is agreed upon.

6.3.1.1.1 Execute IAC Implementation Plan

The ISSE reviews the approved IAC Implementation Plan for clarity and any comments that may have been added by the CA or DAA. The purpose of the IAC Implementation Plan is to provide system developers with the information required to design IAC compliance into a system. If any changes to the overall design of the system have occurred since the IAC Implementation Plan was submitted for review, the ISSE incorporates those changes in the plan.

During system development, the PM/SO/ISSE executes the IAC Implementation Plan, ensuring that the required IACs are incorporated and implemented correctly. The ISSE or IAM works closely with the system architects, engineers, and developers to translate IACs into actionable terms and tracks the implementation of all controls as the system is being developed. The ISSE is the development team's principal advisor and SME on security matters. It is the ISSE's and developers' responsibility to ensure that the IAC Implementation Plan is detailed enough to address how each IAC will be built into the system in order pass an evaluation. If an IAC cannot be properly or completely implemented as planned due to system design changes, the ISSE must make modifications to the IAC Implementation Plan and coordinate the proposed modifications with the CA and DAA if there is a significant change to the security posture.

The goal of this activity is to implement the approved plan to the fullest extent possible.
By approving the plan, the CA and DAA agree that the system will achieve accreditation if the system is developed according to the plan and tests indicate compliance with the plan.
Any changes to this plan will be coordinated and documented to ensure that the CA and DAA concur with them or with the mitigating actions implemented as a result of the changes.

Through monitoring and tracking the implementation of IACs, the ISSE helps the PM ensure that not only the IAC implementation but the overall system development stays on schedule.

6.3.1.1.2 Verify Incorporation of IACs

As system development progresses, the ISSE continues to work with the system engineers and developers. As soon as practical, the ISSE should conduct a verification test on each IAC implementation action that is completed by running the specified test from the Validation Plan and Procedures. In most cases, the earlier that a discrepancy is identified, the easier it is to correct. If any control doesn't pass testing, corrective actions should be accomplished as soon as possible to avoid possible snowball effect with other controls. As with any test, results should be thoroughly documented and the test should be re-run following any corrective action.

As the system development progresses, changes may be made to the design that impact how the IACs will be validated. The ISSE must keep the IAC Implementation Plan current and synchronized with the Validation Plan and Procedures as the system develops. The ISSE should periodically review the Validation Plan and Procedures to ensure that any and all changes to the system and the IAC Implementation Plan are reflected and that all test procedures will remain effective for the validation of applicable IACs.

As much as possible, these tests should be conducted iteratively throughout the system's development to ensure that:

- The system will conform to all IACs at the end of development.
- The IAC Implementation Plan remains current.
- The IAC Validation Plan and Procedures remains current and in synch with the IAC Implementation Plan.
- All test results are documented.
- All changes that affect the IA posture are coordinated with the stakeholders.
- There are no surprises during the validation stage.

6.3.1.1.3 Is Corrective Action Needed?

Throughout the system development process, if no corrective actions are required, the ISSE continues to monitor, test and document as above. If discrepancies are identified during the exercise of the validation procedures, the ISSE collaborates with the system developers to work through any corrective actions necessary to ensure IAC compliance. The particular IAC, size and nature of the discrepancy, and the corresponding corrective action will drive the extent of the coordination that may be necessary. Regardless of action taken, any change to the IAC Implementation Plan and Validation Plan and Procedures must be documented and, if necessary, coordinated with the DIACAP Team.

6.3.1.1.4 Update DIP

If any corrective action was necessary as discussed above, the ISSE should review the DIP and identify any other sections that may require updating to reflect modifications or changes to the system. For example, the system architecture diagram may need to be updated, the hardware or software list may require updating, or even the ports, protocols, or services may need to be updated to reflect the changes in the evolving system.

After the DIP, including the IAC Implementation Plan and the Validation Plan and Procedures, is updated, the development team resumes incorporating the IACs in accordance with the modified IAC Implementation Plan in an iterative fashion until development is complete and the system is ready for formal testing. The ISSE ensures that the corrective actions are successful in addressing the IAC implementation and that all documentation is accurate.

6.3.1.1.5 Prepare System/Site/Environment for C&A Testing

When no further corrective action is required and the ISSE is satisfied that the system is ready for IAC validation testing, the ISSE conducts a final check of all documentation and the system status to verify that the system/site/environment is prepared for testing by the independent Validator. This includes checking the system test environment for integrity, system configurations, availability of all necessary services to support security testing, and completeness and organization of supporting documentation. C&A testing has a cost, both in terms of cost of the Validator and the impact to system availability and other personnel to support the test. Proper prior planning and ensuring that everything is ready prior to the test minimizes the impact of the test to the system, minimizes discrepancies discovered during the test, and minimizes overall costs to the program. At a minimum, the ISSE or IAM should:

- Confirm that the system and environment configurations are in accordance with the DIP, network boundaries are established and controlled according to the accreditation boundary, all operating systems have been properly configured according to established DoD guidelines, and all safety and physical security features applicable to system validation testing have been installed and implemented.

- Review the Validation Plan and Procedures to identify all documents and artifacts that are required to facilitate and support the IAC validation testing, and arrange them for easy access. The Validator will request to see them during the validation test.

- Review the test readiness status, and double check that the system and environment are properly configured with the identified hardware and software, all documents and supporting artifacts are available, and appropriate support personnel are scheduled to be on site during the scheduled validation test.

While these final preparations are in progress, the ISSE and PM should negotiate a testing start date with the Validator. All preparations should be complete by the testing start date.

The ISSE should confirm the system's or program's test-ready status and test dates with the CA.

6.3.1.1.6 Assign Validator

Upon receipt of the ISSE notification that a system will be ready for testing, a Validator is selected and scheduled.

The Validator should be selected according to area of expertise and availability. The Validator will coordinate details for the validation test with the PM/ISSE/IAM. Details include confirming the date and location of testing, facility access requirements, if any, and access to "read-ahead" material the Validator may require prior to conducting the test.

6.3.1.2 Validate Implementation of IACs

Once the Validator has been identified and the System/Site is ready for validation, they will complete the following to support the validation:

- Become familiar with the System/Site by reviewing the C&A Plan.
- Identify and fix any issues with the Validation Plan and Procedures.
- Execute the Validation Plan and Procedures.
- Compare the test results against the expected results to identify any discrepancies/vulnerabilities.
- Determine the severity of these vulnerabilities and which can be fixed quickly.
- Compile the test results for the system/site so the stakeholders can determine how the system/site should proceed in the event that unmitigated vulnerabilities are discovered.

If the Validator feels that additional procedures not identified in the Valuation Plan and Procedures are necessary, the Validator will add these additional procedures into the Validation Plan and Procedures. If a collaboration meeting is required to resolve any issues associated with such actions, then the collaboration meeting will be held.

6.3.1.2.1 Review of the IAC Implementation Plan and the Validation Plan and Procedures

Prior to the on-site validation test, the Validator receives the DIP from the PM/SO/ISSE and reviews all components. The purpose of this review is to provide familiarization with the system itself and prepare for the execution of the validation test. The Validator must understand the functionality and design of the system in order to determine whether the validation procedures have been thoroughly and adequately developed.

6.3.1.2.1.1 Validator reviews the C&A Plan

The C&A Plan component of the DIP covers all the basic system information and should provide the Validator a sufficient understanding of the architecture and design of the system. This section contains descriptions of all related hardware and software; all interfaces, including ports, protocols, and services; the system architecture and accreditation boundary; and all system information required to understand system security requirements. Simply put, this provides the Validator the overall “big picture” of the system about to be tested.

6.3.1.2.1.2 Validator Becomes Familiar with the IAC Implementation Plan

Once the Validator understands the system design, they review the IAC Implementation Plan to understand how the applicable IACs have been incorporated into the system to achieve compliance, which IACs are inherited/inheritable, and what software and/or devices will need to be tested in order to determine compliance levels. The review of the IAC Implementation Plan is cursory but helps to enhance the Validator’s comprehension of the system’s security design, and to check that the security design is appropriate to minimally comply with applicable IACs. If the Validator identifies an obvious inconsistency or finds a potential problem area with the

incorporation of the IACs, the Validator makes a note of it and contacts the PM/SO/ISSE for clarification upon completion of the review.

6.3.1.2.1.3 Validator Pulls Scorecard

The Validator pulls the Scorecard from the https://www.fleetforces.navy.mil/netwarcom/navycanda/default.aspx link for new systems, or from the Comprehensive C&A package for existing systems. For the Marine Cops, this is accomplished via the Xacta tool. It is now a starting point and will be completed after execution of the Validation Plan and Procedures. Enclosure (11) describes the Scorecard template. If not already updated automatically through the tailoring and refinement process when developing the IAC Implementation Plan, the Scorecard may have to be adjusted to match the required IAC compliance requirements so that all results from the validation test are properly captured. This is particularly true for IACs that were added above the baseline IACs based on specific requirements. The IACs on the Scorecard should match those of the DIP line for line.

6.3.1.2.1.4 Validator Reviews Validation Plan and Procedures

The Validator reviews the Validation Plan and Procedures to see what testing is required for validation. After reviewing the other components of the C&A Plan, the Validator should understand how the system was designed and how the IACs were implemented to provide an adequate level of security. The Validation Plan and Procedures should be applicable to the system design and appropriate for the comprehensive validation of IACs. The Validator verifies synchronization and consistency between the IAC Implementation Plan, the Validation Plan and Procedures, and the Scorecard. Finally, the Validator ensures that validation procedures are suitable, repeatable, and executable to verify compliance of system security requirements.

The Validator verifies that all IACs noted as Not Applicable are satisfactorily justified, and reviews the inheritance relationships to see that all are fully documented and appropriate.

6.3.1.2.2 Does the Validation Plan and Procedures need Corrective Action?

After completing the review and documenting any concerns, the Validator determines if the Validation Plan and Procedures can be executed as written or if corrections are necessary. If testing can be conducted, then the scheduled test is confirmed and any comments on the DIP are forwarded to the PM/SO/ISSE. If the Validation Plan and Procedures require adjustments or corrections before the test can be executed, the Validator contacts the PM/SO/ISSE to discuss any recommended corrections or changes. The purpose of the recommended changes is to assist the PM/SO in achieving a successful validation of applicable IACs in one test and to avoid the cost of retesting because of problems in the test plan.

After discussion, the Validator and ISSE/IAM agree on what corrective actions are required and a timeline for their completion. If there is disagreement on a course of action, other DIACAP team members, such as the PM or CA, may be requested to participate in the discussion to resolve the issue.

If adjustments or corrections to the Validation Plan and Procedures are necessary, the ISSE makes the changes as agreed during the discussion and the Validator reviews these changes and

once again determines if the test can be executed. When there are no more required changes, the Validator moves on to Executing the Validation Plan and Procedures.

6.3.1.2.3 Execute the Validation Plan and Procedures

When the Validator is satisfied that the Validation Plan and Procedures are sufficient for test execution, the scheduled validation test is confirmed. The Validator advises the PM/SO/ISSE of any requirements in preparation for the test, such as required documentation that must be available, and prepares the Initial Validation Report Materials for capturing test results.

6.3.1.2.3.1 Validator Conducts Tests and Evaluation to Validate IACs

Upon arrival, the Validator must be allowed access to all system components to be tested for IAC compliance, and must be provided all associated materials required in order to complete the testing. The Validator executes the Validation Plan and Procedures to test and evaluate the system for IAC compliance by accomplishing each test procedure. The ISSE or IAM must be available to answer questions and provide supporting artifacts as required by the Validator.

6.3.1.2.3.2 Validator Documents Raw Test Results

The Validator documents the actual results of each test in the Initial Validation Report at the completion of each Validation Procedure. The actual results should be recorded accurately and any unexpected result should be documented with comments or conditions. The Validator should keep the test report under their personal control at all times. If the validation tests extend overnight or there are interruptions in the test process, the validation report with test results should be locked in a location accessible only to the Validator.

6.3.1.2.4 Compare Validation Test Results to Expected results

When the Validator has completed the testing, and documented all the results in the initial Validation Report, the actual test results must be compared with the previously documented expected results.

The Validator reviews and analyzes the recorded actual raw test validation results to verify that they are as they were documented and have not been modified by any other person.

The Validator compares the actual results to the expected results in the Validation Plan and Procedures. The Validator looks for actual results that did not meet expected results and examines any discrepancies to ensure the validity of the test procedure and its execution.

The Validator identifies all discrepancies between actual and expected results and annotates them for future analysis. Any that are of medium or high vulnerability are marked as items of concern. Each IAC has an associated, pre-defined vulnerability rating that gets assigned if the system is not compliant with the IAC.

6.3.1.2.5 Perform IAC Gap Analysis

The Validator conducts a gap analysis on all discrepancies to determine the cause of the differences between the actual and expected test results. The Validator may be able to discern the cause or they may need to collaborate with the PM/ISSE to determine the reason for differences. A collaborative effort is taken to resolve any issues and concerns, both those that can be readily rectified and those that will require more resources to complete.

The Validator checks all findings against the system architecture to determine whether vulnerabilities identified are actual vulnerabilities to the system or network, or the architecture may have contributed to an erroneous result. Reviewing the system architecture again aids the Validator in understanding and evaluating anomalies in the test results.

6.3.1.2.5.1 Validator identifies any false positives or misleading test results

All findings must be analyzed for validity and accuracy. In some cases, a finding may indicate a condition that does not pose a vulnerability to a specific architecture. This finding would be considered misleading. Also possible is a finding that would be identified as a false positive if there were mistakes in test execution or test procedures, or if automated scanners were used that reported erroneous values such as Telnet running when it is actually disabled.

For each false or misleading finding, the Validator documents the conditions, explanations, or rationale for not achieving the expected result. In some cases, the test procedure may be executed again to verify the conditions or result. All comments are carefully and completely recorded in the Validation Report.

6.3.1.2.5.2 Validator identifies and/or assigns Impact Codes

After all failed IACs have been identified, the Validator notes the pre-assigned Impact Code assigned by the DoD DIACAP Technical Advisory Group (TAG). The impact codes for all IACs are recorded on the Scorecard. If a service unique IAC has been developed with the associated impact code, the results of the service unique IAC must also be recorded on the Scorecard. Upon completion of Scorecard updating, the Validator schedules a meeting to collaborate with the ISSE on mitigating factors for any non compliant IACs. Impact codes are categorized as high, medium or low depending on the consequences of a non-compliant IAC, or in other words, the impact to the system if the IAC is exploited. Taken in conjunction with the severity category, explained in section 6.3.2.3, it helps indicate the urgency with which corrective action should be taken. Definitions for the various Impact Codes are:

- **High Impact Code**: The absence or incorrect implementation of the IAC may have a *severe or catastrophic effect* on system operations, management, or information sharing. Exploitation of the weakness may result in the *destruction* of information resources and/or the *complete loss* of mission capability.

- **Medium Impact Code**: The absence or incorrect implementation of the IAC may have a *serious adverse effect* on system operations management, or information sharing. Exploitation of the weakness may result in *loss* of information resources and/or the *significant degradation* of mission capability.

- **Low Impact Code**: The absence or incorrect implementation of the IAC may have a *limited adverse effect* on system operations, management, or information sharing. Exploitation of the weakness may result in *temporary loss* of information resources and/or *limit the effectiveness* of mission capability.

6.3.1.2.5.3 Validator and ISSE determine fixes & mitigations for vulnerabilities

The Validator and ISSE review all vulnerabilities and determine whether there are any vulnerabilities that could be quickly fixed or any other mitigating measure can be put in place that would reduce the risk of exploitation. All mitigating measures are identified and documented. If mitigations are identified that will reduce the risk, but are not yet applied, they must be scheduled to be applied as soon as possible. They will not affect a reduction in the current risk level of the vulnerability (impact code), but will have a contribution to possibly lowering the severity category rating later. Any fixes that can be completed quickly while the Validator is still on site should be executed immediately so they can be re-tested prior to the Validator departing. If fixes are required, the ISSE and PM need to determine the root cause in order to refine the configuration, installation or other procedures to resolve the discrepancies in the test procedures.

6.3.1.2.5.4 Are there unmitigated medium or high risk vulnerabilities?

After all fixes and mitigating measures have been identified and those that can be applied have been, the Validator reviews the remaining vulnerabilities and Impact Codes. Packages with vulnerabilities mitigated to low risk can now have the Validator begin mapping vulnerabilities to IACs.

For packages with medium or high risk vulnerabilities identified in the test report (as indicated by the vulnerability Impact Codes), and where no mitigations have been identified, or the mitigations have been identified but are not yet applied, the PM must be notified. The Validator notifies the PM/ISSE of the elevated risk levels that may prohibit DAA approval of the package.

6.3.1.2.5.5 PM Collaborates with Stakeholders on Course of Action

If the testing reveals that the site/system has elevated risk levels, the PM and ISSE will schedule a collaborative discussion with the stakeholders to determine what course of action will be taken for each unmitigated medium or high-risk vulnerability. Without collaboration and agreement from the CA and DAA, the likelihood of certifying and accrediting a system with significant risk is extremely unlikely. Packages with medium or high vulnerabilities require the agreement of stakeholders, particularly the DAA, that the risk level can be accepted based upon the balance of vulnerabilities, costs of correction and operational need. The PM/ISSE must schedule a stakeholder meeting to discuss the vulnerabilities of the system in conjunction with its intended architecture and environment. Mission criticality, user needs, defense in depth, security safeguards and other mitigating actions or countermeasures will be factors in determining the acceptance of risk for sites/systems.

For packages with elevated risk, an agreement must be reached on the course of action. Either the package will be acceptable at its current risk level, or it will require additional corrective

action to further reduce the risk to a level that is acceptable to the DAA. These corrective actions will be decided and agreed upon during the collaboration meeting, along with a reasonable timeline for their completion. If the system requires correction, the process reverts back to revising and executing the IAC Implementation Plan. Once the risk level has been determined the Validator can map the vulnerabilities to IACs.

6.3.1.2.5.6 Validator Maps Vulnerabilities to IACs

Where there is more than one vulnerability per IAC, the Impact Codes from all vulnerabilities associated with that IAC need to be rolled up into one code for that IAC. This would happen when many different tests are required for one IAC, such as performing the multitude of tests required by the Gold Disk. By default, the Validator will assign the impact code for the highest vulnerability being rolled up as the overall impact code for that IAC.

The Validator also documents all identified fixes and mitigations required to be applied to the non-compliant IACs as part of the validation report. These are actually recommendations for quick fixes or recommendations to the PM for IT Security POA&M action items. A determination of when fixes and mitigations can be accomplished is also documented.

6.3.1.2.6 Determine if there are Immediate Fixes Possible

The Validator and PM/ISSE determine if an immediate fix is possible to meet the non-compliant IACs. If it has been determined that an immediate fix is possible to reduce risk, the corrective action is scheduled to be implemented (or is directly implemented) by the development team. The ISSE adjusts the IAC Implementation Plan, if required, to show the correction and also updates the Validation Plan and Procedures as appropriate. The development team will use the IAC Implementation Plan to apply the corrective action. These changes are then given to the Validator to again review and run specific Validation Procedures to validate compliance with the applicable IAC. The Validator must evaluate that these changes will not impact the rest of the validation testing. The Validator may determine that full testing must be accomplished after changes have been made. If the changes correct the vulnerability, the IAC can be marked as compliant provided there are no other vulnerabilities associated with that IAC.

If an immediate fix is not possible, the vulnerability will be included in the final version of compiled test results in the Validation Report.

6.3.2 Compile the Test Results

6.3.2.1 Compile Test Results

The Validator compiles the Validation Report by documenting the final results of the Validation Plan and Procedures testing. The Validation Report is the final product of the Validator's efforts and includes the following:

- Test results.
- Risk analysis for each IAC if there are vulnerabilities.
- Recommendation for IT Security POA&M items.

The first step in creating the Validation Report is to capture the final test results, which includes the after corrective action (quick fix) test results, if fixes were applied during the test period. The Validation Report will be updated later with risk analyses and IT Security POA&M recommendations.

The Validator updates the Validation Report with all of the final results of the Validation Tests. The Validation Report now reflects the final compliance status with applicable IACs. The subsequent risk analysis will be based on these results.

6.3.2.2 Develop Scorecard

The Scorecard is a formal compilation of IAC compliance status for the system and provides a quick overview of IAC compliance. Using the Scorecard that was previously started in step 6.3.1.2.1.3, the Validator populates the Scorecard with the IAC Compliance status. For each applicable IAC that has been validated to be in compliance, a "C" is entered in the column for compliance status. For any IAC for which a vulnerability has been identified, an "N/C" is entered in the column. The Scorecard is then saved as the part of the C&A package that will be forwarded to the CA and DAA.

6.3.2.3 Make Residual Risk Assessments

For each IAC, a risk analysis is performed and is recorded as a severity category code. Severity categories are also categorized as CAT I, CAT II, and CAT III. Severity categories are assigned after considering all possible mitigation measures that have been implemented within system design and architecture limitations for the DoD IS in question. An example of a way to determine vulnerability severity category is to use the DISA Security Technical Implementation Guides (STIGs) or site/system scanning tools. Most of the vulnerabilities identified in the STIGS have a related IAC, but in those instances where the IAC has not been identified, it is the Validator's responsibility to identify the appropriate IAC. Most scanning tools do not relate vulnerabilities to IACs and this relationship must be identified by the Validator. Severity categories are expressed as a Category (CAT) number:

- **CAT I**: Assigned to findings that allow primary security protections to be bypassed, allowing immediate access by unauthorized personnel or unauthorized assumption of super-user privileges. An ATO will not be granted while unmitigated CAT I weaknesses are present.

- **CAT II**: Assigned to findings that have a potential to lead to unauthorized system access or activity. CAT II findings that have been satisfactorily mitigated will not prevent an ATO from being granted.

- **CAT III**: Assigned to findings that may impact IA posture but may not be required to be mitigated or corrected in order for an ATO to be granted.

If there are no vulnerabilities identified, there is no residual risk assessment to be conducted and the Validator skips to completing the Validation Report step.

Each vulnerability is analyzed and evaluated to determine the likelihood of exploitation and the extent of potential damage inflicted if the exploitation is successful. The CAT codes assigned by

DISA for generic vulnerabilities are the starting point for vulnerability analysis. Like Impact Codes, Vulnerability CAT codes may be assigned by the Validator if none have been previously assigned.

The Validator assesses the preliminary risk for each vulnerability that has been identified. Mitigating actions (outside the scope of the particular IAC) may reduce the risk level and thereby reduce the severity code assessment. The Validator reviews the documentation of the mitigation discussions to ensure that mitigating factors are considered in the severity code evaluation. If no mitigations have been applied to reduce the risk, the Validator assigns the severity codes without reduction.

If there are any mitigation measures applied to reduce the risk, the Validator determines the impact of the mitigation on the risk for each vulnerability. If the mitigations have been effectively applied, they may reduce the risk by at least one level. However, depending on the mitigation measure and the specific vulnerability, the severity category could potentially be reduced significantly, e.g. from 1 to 3.

As the Validator assigns a severity code to each vulnerability, a written risk analysis is included for each vulnerability explaining the rationale for the severity code evaluation. System architecture and applied mitigating factors are described for their risk reduction impact, and all rationale for risk assignment is documented. IACs with more than one vulnerability are assessed for the impact that the compilation of the vulnerabilities have on the corresponding IAC.

The Validator assigns an overall severity code for each non-compliant IAC, taking into account the severity codes of each associated vulnerability. The Validator then documents the severity code for each IAC in the validation report section of the Validation Plan and Procedures document, by entering the code into the column 12 of the row associated with the corresponding IAC.

For all non-compliant IACs, the Validator documents a recommendation for corrective action to be included in the IT Security POA&M in column 13. An IT Security POA&M entry will be required for all non-compliant IACs.

Once the validation report columns 8 through 14 of the Validation Plan and Procedures document are complete, a copy is delivered to the PM/ISSE for inclusion in the C&A package.

6.3.3 Develop an IT Security POA&M

This section determines if a POA&M is required, and if required, how it is developed, and what is included in it. The template for the POA&M is contained in Enclosure (14) of this handbook.

6.3.3.1 Is an IT Security POA&M Required?

An IT Security POA&M is required to correct all vulnerabilities identified in the validation test and all non-applicable IACs. Only those systems or programs that have a perfect validation report with no vulnerabilities and no non-applicable IACs are not required to develop and submit an IT Security POA&M. Since it is very rare for a system to have no vulnerabilities, an IT Security POA&M will be required in almost all cases.

The ISSE receives the completed Validation Report and Scorecard from the Validator and reviews the recommended actions to be included in the IT Security POA&M. Based on the Validator's results and recommendations, the PM/SO/ISSE or IAM can begin to develop an IT Security POA&M to correct the security discrepancies.

6.3.3.2 Develop an IT Security POA&M

All IACs which are required by the MAC and CL of the system must be accounted for in the IT Security POA&M. Even if vulnerability has been mitigated to a very low risk, it still exists and must be addressed and managed appropriately. If for any reason the mitigation measure were to be removed, the risk level would be returned to its unmitigated level.

All non-compliant, non-compliant inherited and non-applicable IACs must be accounted for in the IT Security POA&M. If any circumstance makes a compliant or inherited IAC become non-compliant (NC), it must be added to the IT Security POA&M to provide visibility, tracking and justification for this status change. If the IAC is inherited, cite the originating IS. For non-applicable IACs, provide the reason the control is non-applicable.

6.3.3.2.1 Determine Actions and Milestones Needed

As with any IT Security POA&M, actions necessary to correct the deficiency are identified, the cost and resources required to implement each action are determined, and an anticipated completion date for each action is estimated.

Every line from the Validation Report that identifies a vulnerability will have a corresponding line in the IT Security POA&M. Starting with the Validator's recommendations, the PM/SO/ISSE or IAM determines what actions are necessary to correct or mitigate each identified vulnerability, along with the estimated resources (including points of contact responsible for managing the action) needed to accomplish the corrective action by the estimated completion date. If vulnerability cannot be corrected, justification must be noted in the IT Security POA&M.

The IT Security POA&M becomes part of the C&A package that will be reviewed by the CA and DAA. It will also exist for the life of the system to manage vulnerabilities and mitigations. The IT Security POA&M is a living document that is managed and updated by the ISSE or IAM on an "as needed" basis. It is reviewed when changes are made, milestones are met or missed, or at a minimum, once per year.

6.3.4 Complete the C&A Package

This section details the steps necessary for the ISSE to compile all the foregoing results and documentation into the final comprehensive C&A package prior to submitting it to the CA.

6.3.4.1 Activity 2 - Implement and Validate Assigned IACs

The ISSE compiles the C&A package by:

- Collecting the various components and artifacts of the C&A package.

- Ensuring that all the components and artifacts of the C&A package are up to date and accurate.
- Reviewing the components and artifacts of the C&A package for quality.

The ISSE/IAM collects the components of the C&A package and ensures that the DIP and SIP are complete and up to date. A review should still be conducted to ensure that documents are current and accurate. ISSE/IAM collects the components of the final DIP, which includes the following minimum components:

- C&A Plan
- IAC Implementation Plan
- Validation Plan and Procedures
- Validation Report
- DIP Concurrence Sheet
- Other accreditation letters

ISSE/IAM updates and completes the DIP by adding the Validation Report, DIP Concurrence Sheet, and any other accreditation letters (if applicable). This updated and completed DIP becomes a key part of the comprehensive C&A package.

ISSE/IAM updates and completes the SIP. This updated and completed SIP is also a key part of the comprehensive C&A package.

The final IT Security POA&M and Scorecard are added to complete the comprehensive C&A package. The SIP, DIP, IT Security POA&M, and Scorecard comprise the comprehensive C&A package and will be reviewed during Certification.

6.3.4.2 C&A Package Quality Review

The certification determination will be made by the CA on the basis of what is contained in the comprehensive C&A package. Every effort should be made to ensure that this package completely and accurately describes the system, its IAC compliance status including all identified vulnerabilities, and all risk mitigation measures taken and planned to allow a thorough and accurate evaluation of the system's risk to be made pursuant to developing a certification determination.

6.3.4.2.1 Perform the final review of the C&A Package for Completeness and Accuracy

ISSE /IAM confirms that the C&A package is complete by ensuring that all the required components of the DIP are included and are up to date, that the SIP is up to date, and that the IT Security POA&M and Scorecard are complete. This package should accurately reflect the system risk. The ISSE/IAM should confirm that all vulnerabilities identified in the testing have been addressed in the IT Security POA&M.

If the C&A Package is not quite ready for submission, the ISSE/IAM gathers, inserts, or updates any missing or incomplete information or makes any necessary changes to ensure the accuracy of the documentation.

6.3.4.2.2 Prepare and Submit C&A Package to PM/SO and UR

When the C&A Package is both complete and accurately reflects the system/program risk, the ISSE or IAM prepares the C&A Package signature page and submits the package for signature. A sample/template for the C&A Package signature page is in Enclosure (10). The same stakeholders that concurred with the DIP in the previous activity will review the final C&A Package.

The ISSE or IAM begins the C&A stakeholder package routing by submitting the C&A Package along with the signature page to the UR and the PM for signature.

6.3.4.3 Sign C&A Package Signature Page

Each of the signatories of the C&A Package has specific actions and responsibilities with regard to their associated items of interest. If the signatories maintained active liaison with the stakeholders throughout the process and conducted all necessary collaboration, they should be able to complete this review quickly and without any delay.

6.3.4.3.1 User Representative and Program Manger Concurrence

The UR and the PM work together to reach concurrence that the C&A Package is ready for submission. This concurrence will be documented with their respective signatures on the C&A Package Signature Page.

The PM/SO should have worked with the UR as necessary throughout system development to ensure that the system capabilities and security controls meet the user needs. It is the PM/SO's responsibility to ensure that the user's functional needs are met and the system is in compliance with DoD IA security standards.

The UR ensures that the IA features of the system do not degrade the required capabilities. If the system meets the users' needs, the UR will sign the C&A Package signature page, indicating concurrence.

If the UR does not concur with the C&A Package, the PM/SO and ISSE/IAM work together to determine a course of action. In some cases, this may send the system back to development and is indicative of a failure to collaborate. If necessary, a discussion with all stakeholders is scheduled by the UR to weigh functionality and IA compliance trade-offs. In those cases, a determination by the CA and DAA should be made before any further action is taken. The PM/SO/ISSE/IAM will document changes in the C&A Package.

The PM/SO is responsible for IA compliance for all systems under their purview. The PM/SO signature is the formal acceptance of responsibility for the accuracy of the content of the C&A Package. If the PM/SO does not concur, the ISSE/IAM completes all directed actions and updates the C&A Package.

When both the PM and UR have signed the signature page, indicating concurrence with the package contents and IA compliance level, the package is forwarded to the Echelon II/MSC for review.

6.3.5 Echelon II/MSC Concurrence of C&A Package

Echelon II/MSC offices, assigned this oversight and resource responsibility, manage the funding requirements, FISMA reporting actions, and supportability and sustainability requirements for systems/programs within their control and responsibility.

6.3.5.1 Echelon II/MSC Evaluation of Supportability and Sustainability Plan

A Supportability and Sustainability plan may be accomplished concurrently with the CA risk determination and the DAA accreditation decision process; however, an ATO cannot be issued without the approved supportability and sustainability plan.

The Echelon II/MSC receives the comprehensive C&A Package from the PM/SO, acknowledges receipt to the PM/SO and UR, and assigns a priority for the package among all the other packages currently under review. As soon as an Echelon II/MSC staff representative is available, the C&A Package is reviewed for life cycle maintenance concurrence.

The Echelon II CIO or the MSC staff representative checks the C&A Package for a life cycle maintenance plan and appropriate supportability and sustainability requirements. The Echelon II/MSC must concur with the supportability and sustainability plans for all systems within their control and responsibility. C&A requires support for the life cycle of the system/program, including annual reviews of IAC compliance and continued monitoring of IA situational awareness.

If the Echelon II/MSC determine that the life cycle maintenance plan is insufficient or not viable for any reason, or the C&A Package has other issues that prevent Echelon II/MSC concurrence, they collaborate with the PM/SO and UR to ensure that the system life cycle management plan will be adequate to maintain the system and its IA requirements throughout its life cycle and to address any issues within the C&A Package.

If changes to the supportability and sustainability plans are required, or there are other issues with the C&A Package that prevent concurrence, the Echelon II/MSC representative collaborates with the Stakeholders to determine the course of action, documents the required modifications, and returns the package and comments back to the PM/SO/ISSE. The PM/SO/ISSE makes the necessary modifications and re-submits the package.

If the plan/package is acceptable and viable, the Echelon II/MSC authority concurs with the C&A Package by signing the C&A signature page and forwards it to the CA, notifying the PM/SO of this action.

6.4 Make Certification Determination and Accreditation Decision

This section describes how the CA and the DAA review a C&A Package and make an overall risk assessment that will lead to a Certification Determination and an Accreditation Decision.

- The CA will determine if the system/site will be certified.
- The DAA will decide if the risk is acceptable by issuing one of the following:
    - ATO
    - IATT
    - IATO
    - DATO

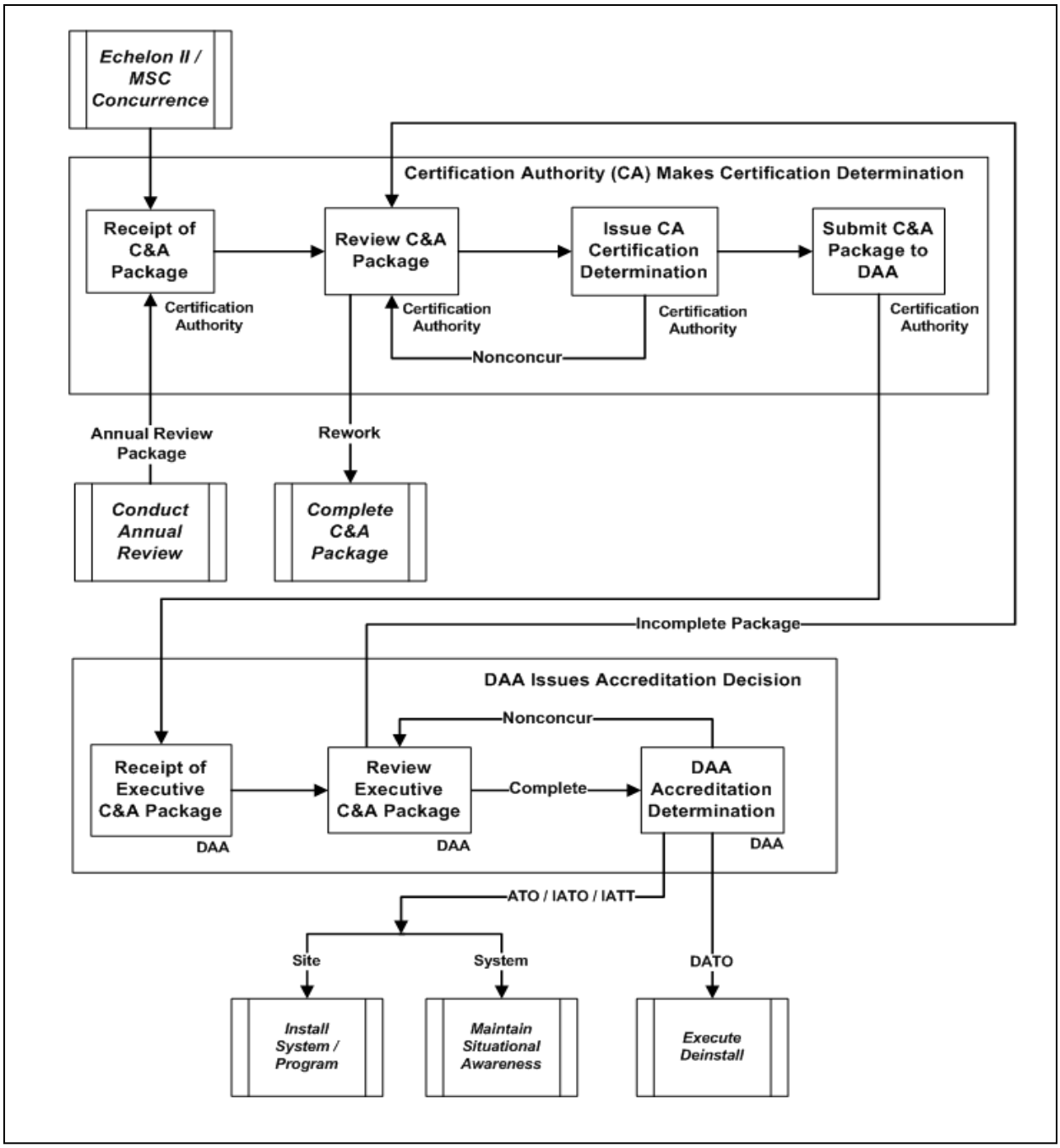


Figure 13. Activity 3 – Make Certification Determination and Accreditation Decision

6.4.1 CA Makes the Certification Determination

Upon receipt of the C&A Package, the CA will acknowledge receipt to the Echelon II/MSC and package PM/SO/ISSE, and prioritize the order in the queue according to their internal CA criteria. The package is assigned to a staff reviewer for analysis and assessment. Ideally, this will be the same staff member that was the POC during all previous collaboration due to their familiarity with the system, but due to workload, this may not always be the case.

6.4.1.1 C&A Package Analysis

For the Navy, the C&A package analysis is accomplished via collaboration of the C&A team. This collaboration is conducted prior to the submission of the package to ensure that all indentified concerns relating to the system have been resolved.

The CA reviewer looks at the quality and the consistency of the package to determine if all information that is needed to make a thorough security evaluation is available. This could be the first look at the package or a re-look if the package was previously returned by the CA or the DAA for more information. A re-look at the package may be required due to a disagreement with the certification determination or when more information is required to make a certification determination.

If the CA reviewer determines that there is insufficient information to make a certification decision, the reviewer assigns error/rejection codes to the package and notifies the CA. A collaboration meeting is then scheduled with the appropriate stakeholders to determine the appropriate course of action. If this meeting determines that the package cannot continue without additional information, the package is returned with comments to the PM/SO/ISSE for correction and re-submission. Notification of this action is sent to Echelon II/MSC and the UR.

If no additional information or rework is required, the package is ready for a detailed evaluation to reach a certification determination.

6.4.1.2 CA Creates the Certification Determination

The CA reviewer examines the Scorecard, Validation Report, and IT Security POA&M to see if there are any vulnerabilities identified. If there are no vulnerabilities, the CA reviewer can start drafting the certification determination.

If vulnerabilities are identified, the CA reviewer analyzes the severity codes that were assigned by the Validator. If the CA reviewer does not concur with the severity codes assigned by the Validator, the CA reviewer annotates the severity codes and documents the justification for the changes.

The CA reviewer makes an overall risk assessment by considering all vulnerabilities, severity codes, system architecture, the intended environment, mitigation/corrective actions contained in the IT Security POA&M, and any modifications to the severity codes that they made.
The overall risk assessment is recorded in the CA Detailed Assessment.

The CA reviewer then drafts the certification determination and accreditation recommendation documents based upon this overall risk assessment. The CA reviewer then submits these with the C&A Package to the CA for concurrence, signature, and forwarding to the DAA.

6.4.1.3 Issue CA Certification Determination

The CA reviews the C&A Package and draft Certification Determination. If the CA does not concur with the certification determination, the C&A Package is sent back to the CA reviewer for further analysis.

If the CA concurs with the reviewer's recommendations, CA signs the Certification Determination document and sends it with the package to the CA Admin.

6.4.1.4 Submit C&A Package to DAA

The CA Admin will create an Executive C&A Package that will be forwarded to the DAA. The Executive C&A Package contains the following components:

- SIP
- Scorecard
- IT Security POA&M
- Certification Determination
- Other required documentation

The CA Admin then forwards the C&A Package to the DAA and notifies the stakeholders that the package has been forwarded. The DAA retains the prerogative to see additional information above that of the C&A Package and will coordinate with the CA to tailor the submitted components as needed. Once CAST is deployed, the DIACAP Team/Stakeholders will have full visibility to all elements in the Comprehensive C&A package. The CA Admin will also notify the stakeholders that the package has been forwarded.

6.4.2 DAA Issues Accreditation Decision

The accreditation decision balances risk to the GIG, operational need to operate, and cost/time to put corrective measures in place. Until now, most of the focus was at the system or enclave level, but the DAA takes a GIG and enterprise view when issuing an accreditation decision.

The DAA admin receives the C&A package, acknowledges receipt to the stakeholders, and prioritizes the order in the queue according to their internal criteria.

6.4.2.1 Analyst Review of Executive C&A Package

A staff analyst is assigned to review the package. Ideally, this will be the same staff member that was the POC during all previous collaboration due to their familiarity with the system, but due to workload, this may not always be the case.

The DAA analyst reviews the C&A package and assesses risk acceptability in light of the operational need for the program/system and the GIG environment it will operate in. All factors are taken into consideration, including the actual vulnerabilities remaining in the system, the criticality of the system, the cost and time to mitigate the vulnerabilities, and the risk they present to the GIG.

If any additional information is required to make an accreditation decision, the DAA analyst details what additional information is required, and sends both the C&A package and the request identifying the required information back to the CA reviewer to respond. If only minor details are needed, a quick collaboration meeting with the cognizant stakeholders could eliminate the need for the package to be returned and allow the accreditation to move forward.

6.4.2.2 Create Draft Accreditation Decision

Once the review is completed, the DAA analyst reviews the draft accreditation decision document, makes any necessary changes, includes the Authorization Termination Date (ATD), and forwards it to the DAA for signature. The accreditation decision will be one of the following types:

- ATO
- IATO
- IATT
- DATO

An ATO accreditation decision must specify an ATD that is within 3 years of the authorization date.

An IATO accreditation decision is intended to allow the system to operate (usually due to criticality of need) while IA weaknesses are managed and rectified. An IATO can be issued for no more than 180 days and may be extended if necessary. Concurrent IATOs may be granted, but may not exceed a total of 360 days.

An IATT is a very limited accreditation decision to support testing using operational data in a test environment or test data in the operational environment which mandates de-installation at ATD unless further operation is authorized by the DAA. A DATO accreditation decision mandates the removal of a system either permanently or until the risk introduced by the system has been mitigated to an acceptable level.

6.4.2.3 Are there any Special Handling Requirements?

If there are no special requirements or any other special program items, the package is forwarded to the DAA for signature.

If the package has special requirements, the DAA analyst forwards the package for review and concurrence. If the package has other special handling or concurrence requirements, it is sent to that program office for their concurrence with the package.

If the special program office does not concur, they document why and return the package to the DAA analyst for additional research. A collaboration meeting is scheduled to determine the course of action to attain accreditation. Once consensus is reached, the package is ready to submit to the DAA.

6.4.2.4 DAA Accreditation Decision

The DAA reviews the Executive C&A package and considers the analyst's overall assessment of risk and their accreditation recommendation. If the acceptance of risk is warranted, the DAA signs the accreditation decision, thereby formally accepting the risk of operating the system. A sample/template of the Accreditation Decision is contained in Enclosure (13).

If more information is required to make a decision, the package is returned to the analyst to coordinate a resolution. This may entail more analysis, a collaboration meeting with the stakeholders, or, in the worst case, returning the package to the CA and maybe the PM/SO for re-work.

6.4.2.4.1 Issue Accreditation Decision

The DAA Admin records the DAA Accreditation Decision, updates appropriate repositories as necessary, and notifies the stakeholders of the decision.

If the Accreditation Decision being issued is a DATO, the next steps are to execute the de-installation procedures found in section 6.5.1.5 for either a system or a site.

If the Accreditation Decision is to issue an ATO, IATO, or IATT, the next steps depend on whether this accreditation is for a system or a site. Systems must be installed at/in sites; therefore the immediately following steps must be performed. Sites will usually skip these steps and move to the Maintain Situational Awareness step below, but they should be familiar with these, since eventually a system will be installed and site personnel will be involved during those events.

6.5 Maintain Authorization to Operate and Conduct Reviews

Upon receipt of the Authorization To Operate (ATO) for the program/system, the program/system can/will be installed in its intended environment with the proper security settings. The IAM will ensure that the task requirements of Maintaining Situational Awareness, conducting Annual Reviews, and Reaccrediting the system/site are met throughout the life cycle of the system. Figure 14 provides a diagram of the various tasks within this DIACAP Activity.

In this section we will cover the detailed tasks to accomplish the following:

- Install the Program/System (applies to system/type accreditations).
- Maintain Situational Awareness.
- Conduct Annual Reviews.
- Reaccredit (every 3 years).

- Accomplish/assist additional evaluation as directed/required.

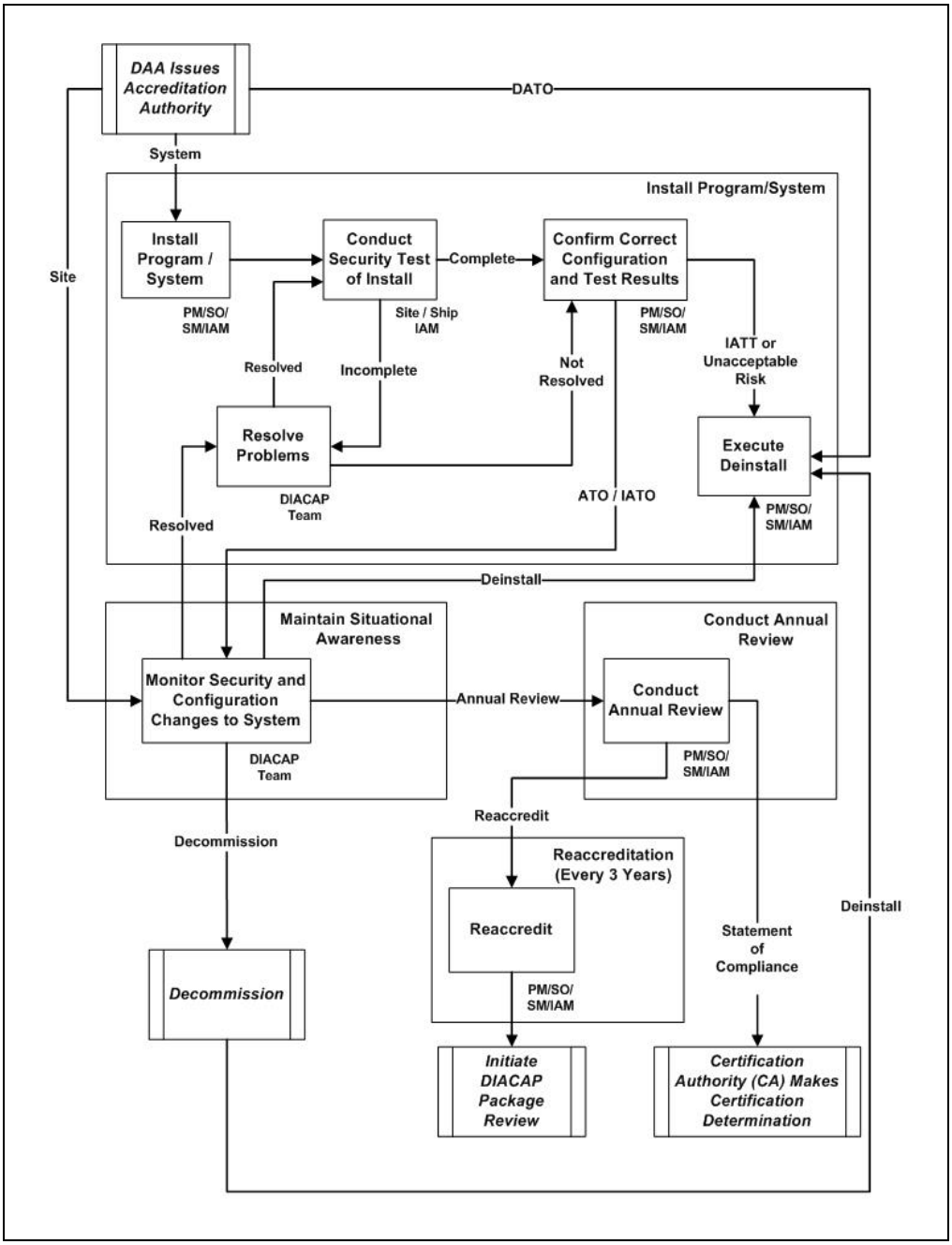


Figure 14. Activity 4 – Maintain Authority to Operate and Conduct Reviews

6.5.1 Install Program/System

With the required ATO, IATO, or IATT, the system is now authorized to be installed and/or connected to a DON accredited environment. Only accredited programs/systems can be installed in accredited sites, networks, environments, or enclaves. For this section of the handbook, installation includes installing the program/system in any environment – including shore site, ship, command, unit, or small field/deployable unit, and the pass-down of IA documentation from the PM/SO to the receiving activity/site.

During these steps:

- The program/system is installed.
- Security testing of the installation is conducted as part of System Operation Verification Test (SOVT).
- Any problems are resolved.
- Correct configuration and test results are confirmed.
- De-install is executed if necessary.

6.5.1.1 PM or SO Installs the Program/System

The PM or SO coordinates and conducts the installation of the program/system at the site, ship, command, or unit, hereafter referred to as the receiving activity. The arrangements include the coordination of time, availability, location, personnel resources, and other details and resources necessary between the PM/SO installation team and the receiving activity to conduct the installation. Both parties must take into consideration the deployment status and the operational tempo of the receiving activity.

The procedures and steps for installing a program/system are beyond the scope of this handbook and will not be covered in detail. The details of the functional installation are the responsibility of the PM/SO. However, the IA steps and procedures that ensure a secure installation are closely related to the functional installation of a program/system. The PM/SO coordinates the various DIACAP steps and procedures below with the receiving activity.

6.5.1.1.1 Provide IA Documentation

The PM/SO installation team provides the receiving activity's IAM with all C&A documentation. Early delivery of this documentation prior to installation ensures better understanding and proper verification of the applicable IACs by the IAM during installation. The documentation includes the system DIACAP package with the SIP, DIP, scorecard, IT Security POA&M, and any other pertinent IA documentation including user and administrator procedures. The Validation Plan and Procedures is required for the receiving activity's IAM to validate the installation of the program/system.

6.5.1.2 Conduct Security Test of Installed System

During these next steps, the secure installation of the program/system is verified. This includes:

- Reviewing the security documentation.
- Conducting the system configuration verification.
- Documenting results.
- Determining compliance.
- Updating the site C&A package.

6.5.1.2.1 Review Security Documentation

The receiving activity's IAM ensures that the complete C&A package is received.
Upon receipt of the security documentation, the IAM reviews the documents to prepare for the local security test to verify the secure installation of the program/system. Reviewing the C&A package security documentation provides an understanding of the security testing requirements and assists the receiving activity to prepare for the testing. Emphasis is on ensuring that the Validation Plan and Procedures is present and that the procedures for validation are understood.

6.5.1.2.2 Conduct System Configuration Verification

The Validation Plan and Procedures should contain all the steps necessary to prepare for and conduct the security verification testing of the program/system configuration. The receiving activity's IAM executes the Validation Plan and Procedures as soon as practical during the functional installation to verify that the system is configured securely and is in compliance with the C&A package and accreditation requirements. The intent of the test is to ensure that the installed program/system is in compliance with the security configuration contained in the IAC Implementation Plan. IACs identified as inherited or inheritable are also verified to determine actual compliance status for the system at the installation site.

Non-compliance with the required security configurations may lead to the introduction of vulnerabilities to the system/program, site, environment, enclave, or GIG. The receiving activity's IAM should coordinate with the PM/SO, CA and DAA as necessary in the event that there are problems encountered in executing the verification.

6.5.1.2.3 Document Results

Compliant and non-compliant results of the testing are documented by the IAM to produce the test results report, which accurately reflects the results of the verification tests. Every effort should be made to address non-compliant security configurations. The Resolve Problem section below contains procedures on resolving non-compliant configuration.

6.5.1.2.4 Is the Installed Program/System In Compliance?

The IAM reviews the results of the security testing, comparing the actual results with the expected results documented in the Validation Plan and Procedures. The IAM must determine if

the system is in compliance with the security configuration as defined in the program/system C&A package. The IAM should obtain help or clarification from the DIACAP team if any confusion is encountered in understanding the IAC Implementation Plan, Validation Plan and Procedures, or test results. However, the primary POC for assistance is the PM.

If the system is in compliance with all of the required security configurations and IACs, the IAM documents these results and updates the site Certification & Accreditation (C&A) Package to reflect the latest program/system installed at the activity. This update should include the results from the Verification tests. Once the Site C&A package is updated, the IAM forwards the results from the Verification tests to the PM/SO. The PM/SO will then update the system documentation to reflect that there was a successful installation at that activity.

If the actual test results differ from those documented in the Validation Plan and Procedures, the system is not compliant with the Security Configuration defined by the C&A package. These differences must be resolved in order to maintain the accreditation of both the system and the site.

6.5.1.3 Resolve Problems

In the event that the verification test revealed that the installed system was not compliant with all the required security configuration requirements defined by the program/system IA documentation and C&A package, the discrepancies must be resolved.

6.5.1.3.1 IAM and/or PM Determine Problem

The IAM and the PM/SO/ISSE analyze the documented results of the verification test to determine the magnitude of problems, discrepancies and vulnerabilities. Possible causes of any deviation from the intended configuration described in the IAC Implementation Plan should be investigated. If the outcome of the investigative effort indicates a trend or systemic problem (vice an isolated incident), the PM/SO/ISSE should revise the procedures for future installations at other activities. If changes to the accredited configuration are necessary, the CA and DAA must be involved for further guidance on analysis and mitigation of the discrepancy and approval of configuration changes. Mission and resources should be considered when determining a solution to mitigate or manage the vulnerability. The findings and results of the analysis are documented by the IAM and PM/SO.

6.5.1.3.2 Can Problems Be Resolved?

As a result of the investigation to determine the cause of the problem, the IAM and the PM/SO/ISSE work together to determine if the problem can be resolved. If the problem can be resolved, the steps are delineated below.

It may be possible that some vulnerabilities cannot be mitigated due to important functional needs. Also, it may not be possible to fully resolve non-compliant configuration due to resource limitations. If the problem cannot be resolved locally, the PM/SO takes responsibility for resolving the issue/problem before the installed program/system can be allowed to operate at that site. The program/system cannot be installed in any other sites until all issues are resolved to the satisfaction of the CA and the DAA.

Coordination with the CA and DAA is required during these resolution steps, as both the certification and accreditation are potentially impacted by configuration changes. Failure to accomplish the coordination results in the invalidation of the accreditation decision. The steps to do this continue below in 6.5.1.4.

6.5.1.3.3 IAM and/or PM Resolve Problem

The IAM and PM/SO/ISSE documents the resolution to mitigate or correct the vulnerability and apply that correction to the installed program/system. If the resolution requires a change in the Validation Plan & Procedures, the IAM and the PM/SO update the program/system C&A package appropriately and repeat the system configuration verification test according to the new procedures.

If the resolution does not require a change to the Validation Plan and Procedures, then the IAM repeats the system configuration verification test to verify compliance.

Upon the completion of the mitigation and/or management of vulnerabilities, the IAM and PM/SO/ISSE ensure that the C&A package of the program/system is updated with the verified corrective actions.

6.5.1.4 Confirm Correct Configuration and Test Results

Following a successful and secure installation at an activity, the PM/SO/ISSE will confirm the correct configuration test results of the installation and update the C&A package to reflect any mitigated vulnerabilities or managed changes that occurred during the installation. This serves to maintain accurate records at the program office as part of the system lifecycle management.

6.5.1.4.1 Review System Configuration Verification Results

The PM/SO reviews the system configuration verification results conducted after the program/system was installed at the site to ensure accuracy and consistency with the C&A package and, if applicable, the type accreditation. From these results, the PM/SO can determine if the procedures for a secure installation are still valid and the Validation Plan and Procedures remain correct. If changes to the program/system security configuration were made during an installation of the program/system, the C&A package must be updated to reflect these changes.

Once the PM/SO/ISSE has determined that the program/system is in compliance with the (accredited) C&A package, the type accreditation is updated to reflect the compliant installation and local records are updated to reflect the activity where the program/system was installed for lifecycle tracking.

6.5.1.4.2 Address Discrepancies

If the program/system is not in compliance, it is the PM/SO responsibility to address the discrepancies. The PM/SO arranges a collaboration meeting with all the stakeholders to determine the course of action to resolve the discrepancy. The severity of vulnerabilities or magnitude of changes to the C&A package, courses of action, time and cost to mitigate or

manage the vulnerabilities and/or changes are to be discussed, and consensus on a course of action will be achieved and documented.

If the courses of action and resolutions result in acceptable risk, the PM/SO/ISSE ensures that the entire C&A package is updated to reflect these latest developments. At a minimum, the IAC Implementation Plan, Validation Plan and Procedures, system configuration, and IT Security POA&M should be reviewed and updated as required, as well as any other applicable artifacts. If necessary, updates should be provided to previously installed sites so those activities can take the appropriate actions.

If the discrepancy cannot be resolved and results in an unacceptable risk, it may be necessary to de-install the program/system. If the program/system is type accredited, the unacceptable risk will likely result in the issuance of a DATO. Follow-up and collaboration with the DAA is required.

6.5.1.5 Execute De-install

De-installation removes a program/system from previously installed activities. This could occur for a variety of reasons, including:

- Program/system has been issued a Denial of Authorization to Operate (DATO).
- The PM/SO should choose to de-install the program/system if that program/system has unacceptable risks or is not operating per the C&A package and/or accreditation.
- Reaccreditation not pursued after the expiration of Authorization To Operate (ATO) or Interim Authorization To Operate (IATO).
- A change in security posture occurs while the program/system is being monitored for security-relevant events.
- Vulnerabilities are discovered during installation that can NOT be mitigated or managed and which pose a risk to the enclave and/or GIG, or corrective action could not be implemented.

Usually, the PM/SO and/or the IAM initiate the action to disconnect or de-install the program/system after collaborating with the DAA. The PM/SO and/or IAM must determine if the system being de-installed is providing inherited IACs. If IACs are being satisfied by the system the site and all systems installed at the site must be notified in order to ensure that the site and/or systems risk is not elevated by the de-installation. Collaboration will occur as required for the determination of the way forward for the site or systems that are affected. The course of action includes changes on the system(s) directly connected to system(s) being de-installed for non type accredited systems with inherited IACs, or de-installation of the program/system at all other site(s) for type accredited systems. All owners of systems that are using the IACs identified as inherited must be notified to determine impact to the systems which are inheriting the compliance status of the IAC. De-install actions are either permanent or the systems remain disconnected until the issues can be corrected and the program/system can be re-accredited.

All courses of action are to be documented in the program/system IT Security POA&M prior to the PM/SO and/or IAM physically disconnecting/de-installing the program/system. Upon

completion of the IT Security POA&M documentation, the PM/SO and/or IAM execute the IT Security POA&M actions and proceed with the disconnection of the program/system.

The PM/SO and/or IAM will generate a Disconnection Statement for submission to the Echelon II/MSC. Once the System Disconnection Statement has been submitted, the PM/SO and/or IAM will then update the program/system and site C&A documentation to reflect the disconnect or de-install actions. This includes updating the SIP. If the program/system will be reaccredited as the same version after correcting the problems or will be accredited as a new version, the PM/SO/ISSE re-enters the process at the beginning of Activity 1.

6.5.2 Maintain Situational Awareness

The activities to maintain situational awareness are the actions performed to maintain accreditation for those program/system or sites that have been issued either an ATO or IATO. The purpose of these actions is to ensure that the integrity of the program/system or site is continually monitored and any deviation from the approved configuration/settings is properly evaluated by the site IAM and/or program/system ISSE. These three monitoring activities are conducted concurrently, or in parallel to each other:

- Monitor for Security Relevant Events.
- Monitor for Life Cycle and Accreditation Status Change.
- Monitor Quality of IAC Implementation.

6.5.2.1.1 Monitoring for Security Relevant Events

When monitoring for security relevant events, the IAM or ISSE monitors the program/system and/or the environment for any security relevant events. This monitoring occurs continuously from accreditation until decommissioning. A security relevant event is any local and/or external change in the environment or program/system that impacts the security posture or IAC compliance of that program/system or site. Some of these events could be:

- Information Assurance Vulnerability Alerts or Bulletins (IAVA/IAVB).
- Any change in compliance with IACs.
- Virus, worm, or other malicious code infection.
- Loss of integrity or confidentiality – unauthorized access.
- Discovered vulnerabilities.
- Inheritance change.
- Boundary vulnerabilities and changes.
- Environment changes.
- Accomplish/assist additional evaluation as directed/required.

Any changes to the security posture, either local or external, are to be documented and assessed for severity. If the event impacts the program/system or the environment, the IAM or ISSE will

determine what risk it has introduced to the program/system, site, enclave, and/or GIG. Collaboration with the CA and/or DAA may be necessary to make this determination. In some cases, very minor or even no corrective action may be needed due to a very low and acceptable risk posed by the event. In this case, the IAM or ISSE will take action, if any is required, and return to continually monitoring the program/system or environment for security relevant events.

If a security event presents an unacceptable risk to the program/system, enclave, or GIG, and the corrective action(s) identified do not require a change of the accreditation, the IAM or ISSE will document and report the event to the stakeholders and execute the corrective action(s). The IAM or ISSE will ensure that the corrective action(s) were effective in mitigating or reducing the risk, will report to the DAA to allow the determination that the risk has been corrected to an acceptable level, and will document the results of the corrective actions that were applied. Corrective actions will be reported to the stakeholders to allow the determination that the risk has been corrected. The ISSE or IAM will then resume monitoring for security relevant events.

If a security event presents an unacceptable risk to the DAA, the program/system, enclave or GIG, and corrective actions identified do not mitigate or manage the vulnerability, the accreditation will be affected. The IAM or ISSE will document and report the event to the stakeholders and the DAA will determine the required actions. Actions may include the shutdown and de-installation procedure described in the Execute De-install section 6.5.1.5 of this handbook.

6.5.2.1.2 Monitoring for Life Cycle and Accreditation Changes

The IAM or ISSE continuously monitors the program/system or the environment for any life cycle and/or accreditation status change from the time of accreditation (or installation) until decommissioning. Any change in the life cycle or accreditation status of the program/system and/or environment will be assessed by the ISSE or the IAM. If a change in the life cycle and/or accreditation status occurs, the IAM or ISSE will collaborate with the stakeholders to determine the course of action that will be taken.

A change in accreditation may be an upgrade, downgrade, or expiration/DATO. If the change is an upgrade, the only action required by the ISSE or the IAM is to receive and document the accreditation change. The ISSE or IAM will then resume monitoring activities.

If the accreditation is a downgraded and corrective action is needed as determined by IAM/ISSE and stakeholder collaboration, the IAM or ISSE will revert back to re-executing the DIP as described in the Execute IAC Implementation Plan section 6.3.1.1.1 of this handbook.

A change in life cycle will result in either the resumption of monitoring activities, re-registration of the program/system, or decommissioning the system. If the life cycle change results in the program/system being decommissioned, the ISSE or IAM will remove the program/system from operation as described in the Decommission Activity section 6.6 of this handbook.

If the life cycle change does not result in decommissioning, the ISSE/IAM and the stakeholders collaborate to determine if the life cycle change impacts the security posture of the program/system, enclave, and GIG. If the change does NOT impact the security posture, the IAM or ISSE will document the change in the program/system's C&A package and resume monitoring

activities. If the change DOES impact the security posture, the IAM or ISSE will re-register the program/system with the DON IA Program as a new version and begin the C&A process for the new version.

6.5.2.1.3 Monitoring for Quality of IAC implementation

The IAM or ISSE continuously monitors for the quality of IAC implementation to ensure that the security functionality they provide continues to be effective. Actions taken may include reviewing the inheritance relationships between systems and/or network, reviewing audit logs, conducting spot audits, conducting vulnerability scans, and checking for changes to the IACs as listed in the DIACAP Knowledge Base. In addition, the IAM or ISSE will also be aware of when the program/system/site is due for its annual review. This monitoring occurs continuously from accreditation until decommissioning.

Because programs/systems and networks are so interrelated, the ISSE/IAM must review all inheritance relationships to ensure that any IACs that are inherited are still valid and provide the required security functionality to the inheriting system.

The ISSE/IAM will also check the latest IAC list (for the system's MAC and CL) from the DIACAP KS and compare it with the program/system's last validation report. If there is no difference, or if the difference between the updated IAC list and the program/system's last validation report does not impact the security posture of the program/system or environment, the ISSE /IAM will resume the monitoring activities. Any difference between the latest IAC list and the program/system's validation report may indicate a change in IAC compliance and must be assessed for a possible change in the program/system or environment's security posture.

If the security posture of the program/system or environment has changed, the IAM/ISSE will re-register the program/system with the DON IA Program and cycle through the C&A process again.

As the program/system/site approaches its 12-month anniversary from accreditation or its last annual review, the IAM/ISSE will initiate the annual review as described below in the Conduct Annual Review section. In maintaining a three-year ATO, annual reviews are conducted for the first two years while reaccreditation is conducted during the third year.

6.5.2.1.4 Shutdown System

In case of emergent circumstances or receipt of DATO, or as a result of monitoring activities, a system/site may need to be shut down. This may be for a short term until problems are corrected, or it may be permanent. When shutdown is warranted, the program/system is disconnected and the IAM/ISSE executes corrective action immediately. If the corrective action resolves the problem, the actions are verified (tested) for effectiveness, the C&A documentation is updated to reflect the action, and normal operations may then be resumed after gaining permission from the DAA.

If corrective action cannot be taken, the IAM/ISSE must then determine if the program/system will be reaccredited or if it will be de-installed. For reaccreditation action, the C&A process starts at the beginning of section 6.2 again. If the program/system will be de-installed, the

stakeholders are notified and the IAM/ISSE should follow the de-install procedures in section 6.5.1.5 of this handbook.

6.5.3 Conduct Annual Reviews

The purpose of the annual review is to ensure that the IA posture of the program/system/site is assessed at least annually and must be documented and reported to comply with DIACAP and FISMA requirements. Programs/systems are reviewed annually at the program office and sites may review installed systems individually or collectively with the site accreditation in accordance with service unique guidance.

6.5.3.1.1 Review IACs

The ISSE/IAM should obtain the validation results for inherited IACs and review them with the rest of the C&A package of the system/site for accuracy. The ISSE/IAM updates the C&A package if any discrepancies are discovered prior to testing and validating.

6.5.3.1.2 Test/Validate Applicable IACs

Once the ISSE/IAM verifies the accuracy of the C&A package, they execute the Validation Plan and Procedure for the program/system or site as applicable. The ISSE/IAM reviews the test results and compares them with the previous (old) test results documented in the validation report portion of the previous Validation Plan and Procedure document of the C&A package. The ISSE/IAM determines if the program/system/site is in compliance with all applicable IACs. If the program/system/site is in compliance, the ISSE/IAM updates the validation report portion in the current Validation Plan and Procedure document in C&A package. If not in compliance, or if a degradation to the IA posture occurred, the ISSE/IAM analyzes the problem and coordinates a solution with the PM, and stakeholders if necessary, which is then documented in the C&A package. The IT Security POA&M will also be updated to reflect the necessary corrective action.

6.5.3.1.3 Compile Annual Review Package

The ISSE/IAM also updates the Scorecard to reflect the new IAC compliance status along with the date(s) conducted. The final step is for the ISSE/IAM to draft a Statement of Compliance; a sample is contained in Enclosure (15).

The Annual Review Package consists of the SIP, Scorecard, IT Security POA&M, and the Statement of Compliance. Once the package is complete the PM/ISSE/IAM signs and submits it to the CA.

6.5.3.2 Reaccredit

If this is the third Annual Review or significant changes have been made to the program/system/site, the ISSE or site IAM compiles reaccreditation C&A package consisting of the following minimum requirements:

- Updated SIP

- Updated DIP
- Updated Scorecard
- Updated IT Security POA&M
- Statement of Compliance
- Signature Page

Once the C&A package is complete, the ISSE/IAM submits it to the SO/PM/Commanding Officer (CO), as appropriate, for signature. Once they approve the package, the package is forwarded to the Echelon II/MSC, CA, and DAA much like the original accreditation.

6.6 DECOMMISSION

Decommissioning is the process to formally remove a program/system from operation, account for all installed instances of it, and remove it from all registries. This ensures that no unauthorized and unsupported "orphan" programs/systems still exist that could introduce unwarranted vulnerabilities into DON and DoD networks and enclaves.

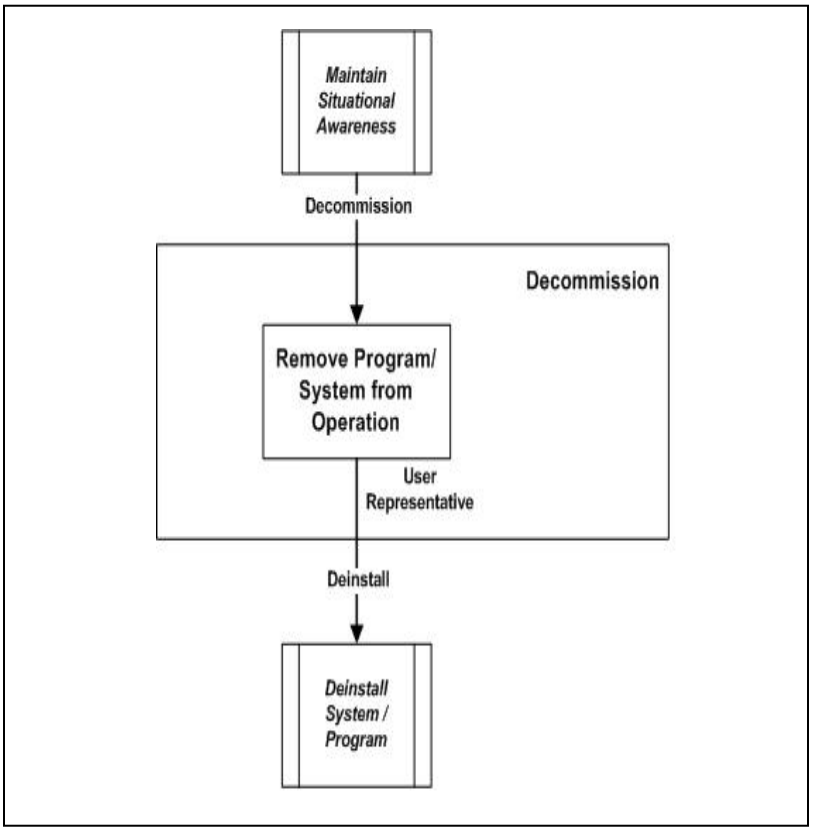


Figure 15. Activity 5 – Decommission

6.6.1.1 Remove Program/System from Operation

A program/system requires removal if it is at the end of its life cycle, it is being replaced by a newer version, it has vulnerabilities that are serious enough to warrant retiring the system, or it has failed to attain accreditation or re-accreditation. Unless previously coordinated and approved by the DAA, removal of a program/system should start at or before the accreditation expiration date.

6.6.1.1.1 Notify Stakeholders of Decommission

Decommissioning starts with the PM updating the C&A documents and notifying the stakeholders of the intent or mandate (as applicable) to decommission the program/system. Notification can by made via email or message. The update to the SIP will convey the intent or need to remove the program/system from operation and all repositories

Inheritance of IAC dependencies must be taken into consideration by the PM/ISSE. In most cases, but not necessarily all, an installed program/system will inherit IAC functionality from the environment or perhaps other installed programs/systems. In this case, removal of the program/ system should have minimal impact. If the program/system being decommissioned contains inheritable IACs that are used by the site or other systems installed at a site, the security posture of those will be impacted by the decommissioning. Understanding the inheritance of IACs between a system and all installed sites is critical and this impact must be evaluated by the PM/ISSE and coordinated with all affected sites and programs. Additional measures may have to be put in place prior to program/system, removal to compensate for the inheritable IACs supplied by the program/system and the C&A package for the remaining site/systems must be updated. Depending on the magnitude of change, IACs and associated risk, these remaining sites/systems may need to submit for reaccreditation. In these cases, the PM/ISSE will need to collaborate with the appropriate stakeholders to determine the appropriate course of action.

Type-accredited systems will normally require an IT Security POA&M to ensure that all tasks and evaluations are conducted at all the installed instances (sites) of the system.

6.6.1.1.2 Decommission Activity

When the Echelon II/MSC receives the decommissioning POA&M, they evaluate it for impact to other operational capability, impact to other systems, and funding resources for the supportability and sustainability of all systems under their control and responsibility. The Echelon II/MSC also updates their records for FISMA reporting. Any adverse impact will be coordinated and rectified with the appropriate parties.

When the CA receives the decommissioning POA&M, a staff reviewer is assigned to assess the risk to the operational environment. The impact of inherited/inheritable IAC functionality and dependencies between systems/sites must be evaluated, as well as the required mitigating countermeasures that must be put in place for the affected programs/systems. Risk could be incurred by the affected sites/systems that impact their accreditation status. Upon completing the impact assessment, the reviewer prepares and submits a decommission impact risk assessment statement to the CA. If the CA does not concur with the statement, it is returned to the reviewer

for further analysis. If the CA concurs, the statement is signed and forwarded with the POA&M to the DAA.

When the DAA receives the decommissioning POA&M and CA's risk assessment, a staff analyst is assigned to assess the risk impact to the operational environment. If there is no impact, the DAA is notified and the PM is receives notification that the program/system can be removed at all installed locations. If there is impact to other sites/systems, the staff analyst drafts accreditation downgrade modifications for the affected ATOs and forwards it to the DAA. If the DAA does not concur, it is returned to the analyst for further analysis and resolution. If the DAA concurs with the downgrade modifications, they are signed and issued to the affected programs/systems. The decommissioning system PM is notified that removal of the program/system can begin.

6.6.1.1.3 Remove from Operation at Registered Places

The PM executes the decommissioning POA&M and coordinates the necessary activities with all installed instances. Any hardware should be properly disposed according to applicable guidelines. It is critical for the PM/ISSE to account for all installed instances of the program/system to prevent "orphan" systems remaining behind. Upon completion of de-installation at all activities, the DAA will issue the DATO accreditation statement.

If an activity must retain the program/system for legitimate operational or business needs, they must coordinate with their Echelon II/MSC and a determination will be made for the assumption of responsibility for maintaining the program/system following decommissioning by the PM. In these cases, the program/system must be re-accredited as a new program/system under the sponsorship/ownership of the site.

ENCLOSURE (1) REFERENCES

(a) Subchapter III of Chapter 35 of title 44, United States Code, "Federal Information Security Management Act (FISMA) of 2002"

(b) DoD Directive 8500.01E, "Information Assurance (IA)," October 24, 2002. (Copies of this document are available online at http://www.dtic.mil/whs/directives/or ASDNII.pubs@osd.mil.)

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

(d) DoD Directive 8100.1, "Global Information Grid (GIG) Overarching Policy," September 19, 2002. (Copies of this document are available online at http://www.dtic.mil/whs/directives/corres/pdf/810001p.pdf.)

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

(f) DoD Instruction 5200.40, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP)," December 30, 1997 (hereby canceled). (Copies of this document are available online at http://www.dtic.mil/whs/directives/corres/ins1.html or ASDNII.pubs@osd.mil.)

(g) DoD Manual 8510.1-M, "Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP) Application Manual," July, 2000 (hereby canceled). (Copies of this document are available at http://www.dtic.mil/whs/directives/corres/html/85101m.htm or ASDNII.pubs@osd.mil.)

(h) Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer Memorandum, "Interim Department of Defense (DoD) Information Assurance (IA) Certification and Accreditation (C&A) Process Guidance," July 6, 2006 (hereby canceled). (Copies of this document are available online at http://iase.disa.mil/ditscap/interim-ca-guidance.pdf.)

(i) Section 11331 of title 40, United States Code

(j) Executive Order 12333, "United States Intelligence Activities," December 4, 1981, as amended. (Copies of this document are available online at http://www.archives.gov/federal-register/codification/executive-order/12333.html.)

(k) DoD Directive 8115.01, "Information Technology Portfolio Management," October 10, 2005. (Copies of this document are available online at https://acc.dau.mil/.)

(l) DoD Directive 8570.1, "Information Assurance Training, Certification, and Workforce Management," August 15, 2004. (Copies of this document are available online at http://www.dtic.mil/whs/directives/ or ASDNII.pubs@osd.mil.

(m) DoD Instruction 5000.2, "Operation of the Defense Acquisition System," May 12, 2003. (Copies of this document are available online at http://www.dtic.mil/whs/directives/corres/ins1.html.)

(n) DoD Directive 8581.1, "Information Assurance (IA) Policy for Space Systems Used by the Department of Defense," June 21, 2005

(o) DoD 5200.1-R "Information Security Program," January 1997. (Copies of this document are available online at http://www.dtic.mil/whs/directives/ or USDI.Pubs@osd.mil.)

(p) DoD 8320.2-G, "Guidance for Implementing Net-Centric Data Sharing," April 12, 2006

(q) Department of Defense (DoD) Chief Information Officer (CIO) Memorandum, Charter, "DISN Security Accreditation Working Group (DSAWG)," March 26, 2004. (Copies of this document available at http://www.iase.disa.smil.mil/dsawg.)

(r) Assistant Secretary of Defense Networks and Information Integration Memorandum, "Charter of the Department of Defense (DoD) Information Assurance Certification and Accreditation Process (DIACAP) Technical Advisory Group (TAG)," July 26, 2007. (Copies of this document available at https://diacap.iaportal.navy.mil/ks.)

(s) Department of Defense (DoD) Chief Information Officer (CIO) Memorandum "Charter of IA Senior Leadership Group," March 5, 2004. (Copies of this document available at https://powhatan.iiie.disa.mil/iasl-iasg/charters.html.)

(t) Appendix III to Office of Management and Budget Circular No. A-130, "Security of Federal Automated Information Resources," (Revised). http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html.

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

(v) DoD 8910.1-M, "Procedures for Management of Information Requirements," June 1998

(w) Committee on National Security Systems Instruction No. 4009, "National Information Assurance (IA) Glossary," as revised June 2006

(x) Joint Publication 1-02, "Department of Defense Dictionary of Military and Associated Terms," as amended

(y) DoD Directive 8320.2, "Data Sharing in a Net-Centric Department of Defense," April 23, 2007. http://www.dtic.mil/whs/directives/corres/pdf/832002p.pdf.

(z) DoD 5400.11-R, "Department of Defense Privacy Program," May 14, 2007

(aa) OMB Memorandum M-04-04, "E-Authentication Guidance for Federal Agencies," December 16, 2003

(bb) OMB Memorandum, "FY 2004 Reporting Instructions for the Federal Information Security Management Act," August 23, 2004

(cc) OMB Circular No. A-11, "Preparation, Submission, and Execution of the Budget," June 2006

(dd) Secretary of the Navy Instruction 5239.3A, "Department of the Navy Information Assurance (IA) Policy," 20 December 2004. This document is available online at http://doni.daps.dla.mil/Directives/05000%20General%20Management%20Security%20and%20Safety%20Services/05-200%20Management%20Program%20and%20Techniques%20Services/5239.3A.pdf.

(ee) Naval Staff Office Publications 5239, Module 5239-13, "Certification and Accreditation Guidebook" and Module 5239-16 "Risk Assessment Guidebook," Sept 1995.

(ff) SECNAV M-5239.1, "Information Assurance Manual," November 2005. Para. 2.4 – Roles and Responsibilities. (Copies of this document are available online at http://www.fas.org/irp/doddir/navy/secnavinst/m5239_1.pdf.)

(gg) CNSSI 4009, National Information Assurance (IA) Glossary, June 2006. (Copies of this document are available online at http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf.

(hh) E-Government Act of 2002 (H.R. 2458/S. 803), 17 Dec 2002. (Explanation available online at http://www.whitehouse.gov/omb/egov/g-4-act.html.)

(ii) DoD Instruction 8580.1, "Information Assurance (IA) in the Defense Acquisition System," 9 Jul 2004. (Copies of this document are available online at http://www.dtic.mil/whs/directives/corres/ins1.html or ASDNII.pubs@osd.mil.)

(jj) DoD Directive 5000.1, "The Defense Acquisition System," 12 May 2003. (Copies of this document are available online at http://www.dtic.mil/whs/directives/corres/dir.html.)

(kk) DoD Instruction S-3600.2, "Information Operations Security Classification Guidance," August 6, 1998. (Copies of this document are available online at http://www.amc.army.mil/amc/ci/matrix/documents/dod/dodi_3600_2.html.)

(ll) CJCSM 6510.01, "Defense-in-Depth: Information Assurance (IA) and Computer Network Defense (CND)," 25 Mar 03. (Copies of this document are available online at http://www.dtic.mil/cjcs_directives/cjcs/manuals.htm.)

(mm) SECNAV M-5510.36, "DON Information Security Program. Manual," 1 Jul 06. (Copies of this document are available online at http://neds.daps.dla.mil/SECNAV%20Manuals1/5510.36.pdf.)

(nn) SECNAV Instruction 5211.5E, "Department of the Navy (DON) Privacy Program," DNS-36, 28 Dec 2005. (Copies of this document are available online at http://doni.daps.dla.mil/Directives/05000%20General%20Management%20Security%

20and%20Safety%20Services/05-200%20Management%20Program%20and%20Techniques%20Services/5211.5E.pdf .

(oo) CJCSI 6211.02B, "Defense Information System Network (DISN): Policy, Responsibilities and Processes," 31 Jul 03 (current as of 30 Aug 06). (Copies of this document are available online at http://www.dtic.mil/cjcs_directives/cdata/unlimit/6211_02.pdf. Specific guidance is provided on the NCDSO web page located at https://infosec.navy.mil/cds/cds_home.jsp.)

(pp) DoD Chief Information Officer Guidance and Policy Memorandum No. 6-8510 "Department of Defense Global Information Grid Information Assurance,"

(qq) CNSSD-500, "Information Assurance (IA) Education, Training, and Awareness," August 2006; Supersedes NSTISSD-500, 25 February 1993. (Copies of this document are available online at http://www.cnss.gov/directives.html.)

(rr) NSTISSI-4011, "National Training Standard for Information Systems Security (INFOSEC) Professionals;" National Security Telecommunications and Information Systems Security, 20 June 1994. (Copies of this document are available online at http://www.cnss.gov/Assets/pdf/nstissi_4011.pdf.)

(ss) CNSSI 4012, "National Information Assurance Training Standard for Senior System Managers," June 2004. (Copies of this document are available online at http://www.cnss.gov/Assets/pdf/cnssi_4012.pdf.)

(tt) DoD 8570.1-M, "Information Assurance Workforce Improvement Program," Assistant Secretary of Defense for Networks and Information Integration/Department of Defense Chief Information Officer, 19 Dec 2005. (Copies of this document are available online at http://www.dtic.mil/whs/directives/corres/pdf/857001m.pdf.)

(uu) Policy Memorandum: DoD Net-Centric Data Strategy – May 9, 2003, by John P. Stenbit. (Copies of this document are available online at http://www.dod.mil/nii/org/cio/doc/Net-Centric-Data-Strategy-2003-05-092.pdf.)

(vv) Clinger-Cohen Act (The Information Technology Management Reform Act of 1996), S1124. (Copies of this document are available online at http://www.cio.gov/Documents/it_management_reform_act_Feb_1996.html.)

(ww) DoDD 8000.1, "Management of DoD Information Resources and Information Technology," 27 Feb 2002. Certified current as of 23 Apr 2007. (Copies of this document are available online at http://www.dtic.mil/whs/directives/corres/pdf/800001p.pdf.)

(xx) 5 U.S.C. Section 552a, "Records about individuals." (Copies of this document are available online at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=browse_usc&docid=Cite:+5USC552a.)

Other Web Links

The entire SECNAV IA manual series may be accessed through the Department of Navy Issuances website: http://doni.daps.dla.mil .

National Institute of Standards and Technology (NIST) publishes primarily the 800-series Special Publications found at http://csrc.nist.gov/publications/nistpubs/.

PIAs must be conducted using the prescribed DON format located at http://www.doncio.navy.mil. PIA information relevant to the Marine Corps C&A process may be found at https://hqdod.hqmc.usmc.mil/pii.asp, and for the Navy at http://www.doncio.navy.mil.

The Navy CDS Office (NCDSO), operated by SPAWAR, provides the Navy interface and representation to this DoD process. Specific guidance is provided on the NCDSO web page located at https://infosec.navy.mil/cds/cds_home.jsp.

IACs and their associated validation procedures can be accessed via the DIACAP Knowledge Service IA Portal at https://diacap.iaportal.navy.mil/.

ENCLOSURE (2) DEFINITIONS

Accountability. Information Security process of tracing IS activities to a responsible source.

Accreditation. Formal declaration by the DAA that an IS is approved to operate at an acceptable level of risk, based on the implementation of an approved set of technical, managerial and procedural safeguards.

Accreditation Boundary. Identifies the information resources covered by an accreditation decision, as distinguished from separately accredited information resources that are interconnected or with which information is exchanged via messaging.

Accreditation Decision. A formal statement by a designated accrediting authority (DAA) regarding acceptance of the risk associated with operating a DoD information system (IS) and expressed as an authorization to operate (ATO), interim ATO (IATO), interim authorization to test (IATT), or denial of ATO (DATO). The accreditation decision may be issued in hard copy with a traditional signature or issued electronically signed with a DoD public key infrastructure (PKI)-certified digital signature.

Acquisition Organization. The Government organization that is responsible for developing a system.

Adequate Security. Security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information. This includes assuring that ISs operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost effective management personnel, operational and technical controls.

Application. Software program that performs a specific function directly for a user and can be executed without access to system control, monitoring or administrative privileges. Examples include office automation, electronic mail, web services, and major functional or mission software programs.

Architecture. The configuration of any equipment, or interconnected system or subsystems of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information; includes computers, ancillary equipment, and services, including support services and related resources.

Artifacts. System policies, documentation, plans, test procedures, test results, and other evidence that express or enforce the IA posture of the DoD IS, make up the C&A (C&A) information, and provide evidence of compliance with the assigned IACs.

Assigned IACs. A list of IACs that a DoD IS must address to achieve an adequate IA posture. Assigned IACs include baseline DoD IACs, optional DoD IACs for special conditions or technologies, e.g., health information portability and privacy or cross security domain solutions, and DoD, Mission Area, Component and DoD IS supplements, if any. DoDI 8500.2. See Enclosure (1), Reference (e).

Assurance. Measure of confidence that the security features, practices, procedures and architecture of an IT system accurately mediate and enforce the security policy.

Augmenting IACs. IACs that augment baseline IACs to address special security needs or unique requirements (e.g., cross security domain solutions, health information portability, privacy, etc.) of the IS(s) to which they apply. Augmenting IACs may originate from a mission area (MA), a DoD Component, a Community of Interest (COI), or a local system. Augmenting IACs must neither contradict nor negate DoD baseline IACs and must not degrade interoperability across the DoD Enterprise.

Automated Information System (AIS). Set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. Includes AIS applications, enclaves, outsourced IT-based processes, and platform IT interconnections.

Authenticity. The property that allows the ability to validate the claimed identity of a system entity.

Authorization Termination Date (ATD). The date assigned by the DAA that indicates the date upon which authorization to operate is terminated for an ATO, IATO, or IATT.

Authorization to Operate (ATO). The authorization granted by a DAA, for a DoD IS to process, store, or transmit information. An ATO indicates a DoD IS has adequately implemented all assigned IACs to the point where residual risk is acceptable to the DAA. Authorization is based on acceptability of the IA component, the system architecture and implementation of assigned IACs.

Automated Information System (AIS) Application. See DoD Information System.

Availability. Timely, reliable access to data and information services for authorized users.

Base Area Network (BAN). A base-area network is a computer network covering a military geographic area, like a post, station, base, or group of buildings e.g. a facility or campus. The defining characteristics of BANs, in contrast to wide-area networks (WANs), include their smaller geographic range.

Certification & Accreditation Support Tool (CAST). The DON DIACAP C&A support system designed to automate the C&A process.

Certification. Comprehensive evaluation of the technical and non-technical security safeguards of an IS to support the accreditation process that establishes the extent to which a particular design and implementation meets a set of specified security requirements.

Certification Determination. A CA's determination of the degree to which a system complies with assigned IACs based on validation results. It identifies and assesses the residual risk of operating a system and the costs to correct or mitigate IA security weaknesses as documented in the Information Technology (IT) Security Plan of Action and Milestones (POA&M).

Certifying Authority (CA). An official responsible for performing the comprehensive evaluation of the security features of an information system and determining the degree to which it meets its security requirements.

Certifying Authority Representative. Official acting on behalf of the CA.

Circuit. A conglomeration and interconnection of electronic components with a number of channels to provide a communication path or network for one-way or two-way communications. Usually a pair of channels providing bidirectional communication. More or less interchangeable with "network".

Community of Interest (COI). An inclusive term used to describe collaborative groups of users who must exchange information in pursuit of their shared goals, interests, missions, or business processes and who therefore must have shared vocabulary for the information they exchange. COIs in the DoD can be either institutional or expedient. Institutional COIs, whether functional or cross-functional, tend to be continuing entities with responsibilities for ongoing operations. Expedient COIs are more transitory and ad hoc, focusing on contingency and crisis operations. "DoD Net-Centric Data Strategy," see REFERENCES (uu), addresses institutional and expedient COIs.

Community Risk. Probability that a particular vulnerability will be exploited within an interacting population and adversely impact some members of that population.

Computing Environment. Workstation or host (server) and its operating system, peripherals and applications. The environment includes physical, administrative, and personnel procedures as well as communication and networking relationships with other ISs.

Confidentiality. Assurance that information is not disclosed to unauthorized persons, processes, or devices.

Confidentiality Level (CL). Applicable to DoD ISs, the confidentiality level is primarily used to establish acceptable access factors, such as requirements for individual security clearances or background investigations, access approvals, and need-to share determinations; interconnection controls and approvals; and acceptable methods by which users may access the system (e.g., intranet, Internet, wireless). The DoDI 8500.2 See REFERENCES (e.) defines three confidentiality levels: classified, sensitive, and public.

Configuration Control. Process of controlling modifications to hardware, firmware, software, and documentation to ensure that the system is protected against improper modifications prior to, during, and after system implementation.

Configuration Management (CM). Management of security features and assurances through control of changes made to hardware, software, firmware, documentation, test, test fixtures, and test documentation throughout the life-cycle of an IS.

Configuration Manager. The individual or organization responsible for Configuration Control or CM.

Data Integrity. Condition existing when data is unchanged from its source and has not been accidentally or maliciously modified, altered or destroyed.

Defense Information Infrastructure (DII). The DII is the seamless web of communications networks, computers, software, databases, applications, data, security services, and other capabilities that meets the information processing and transport needs of DoD users in peace and in all crises, conflict, humanitarian support, and wartime roles.

Denial of Authorization to Operate (DATO). DAA determination that a DoD IS cannot operate because of an inadequate IA design, failure to adequately implement assigned IACs, or other lack of adequate security. If the system is already operational, the operation of the system is halted.

Designated Accrediting Authority (DAA or Accreditor). Official with the authority to formally assume the responsibility for operating a system or network at an acceptable level of risk. This term is synonymous with authorizing official, designated approving authority and delegated accrediting authority.

Developmental Designated Accrediting Authority (DDAA). The DDAA is the official responsible for ensuring completion of the DAA function of C&A for applications or systems during acquisition, development, Certification Test and Evaluation (CT&E) and risk mitigation prior to use or testing within the operational Naval enterprise.

Developer. The organization that develops the IS.

DIACAP Implementation Plan. The Implementation Plan contains the IS assigned IACs. The plan also includes the implementation status, responsible entities, resources and the estimated completion date for each assigned IA Control. The plan may reference applicable supporting implementation material and artifacts.

DIACAP Knowledge Service. A web-based repository of information and tools for implementing the DIACAP that is maintained through the DIACAP Technical Advisory Group (TAG).

DIACAP Package. The collection of documents or collection of data objects generated through DIACAP implementation for an IS. A DIACAP package is developed through implementing the activities of the DIACAP and maintained throughout a system life cycle. Information from the package is made available as needed to support an accreditation or other decision such as a connection approval. The two types of DIACAP package are the Comprehensive Package, containing all information connected with the certification of the IS, and the Executive Package, containing minimum information for an accreditation decision. The Comprehensive Package contains the SIP, the DIACAP Implementation Plan, the Certification Documentation, the DIACAP Scorecard, and the IT Security POA&M if required. The Executive Package contains the SIP, the DIACAP Scorecard, and the IT Security POA&M if required.

DIACAP Scorecard. A summary report that shows the certified or accredited implementation status of a DoD IS assigned IACs and supports or conveys a certification determination and/or accreditation decision. The DIACAP Scorecard is intended to convey information about the IA posture of a DoD IS in a format that can be easily understood by managers and be easily exchanged electronically.

DIACAP Team. The officials responsible for implementing the DIACAP for a DoD IS. At a minimum the DIACAP Team includes the DAA, the CA, the SIAO, the DoD IS PM/SO or SM, the DoD IS IAM, IAO, and a User Representative.

DoD Information Assurance Certification and Accreditation Process (DIACAP). The DoD life cycle processes for identifying, implementing, validating, certifying, and managing IA capabilities and services, expressed as IACs, and authorizing the operation of DoD ISs in accordance with statutory, Federal and DoD requirements.

DoD Information System. DoD set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information.

DoD Information Technology Portfolio Repository. Department of the Navy DITPR-DON is the DON variant of DoD IT Portfolio Registry (DITPR) that is used to record investment review and certification submission information, FISMA assessments, E-Authentication status, and Privacy Impact Assessment status.

DoD Information Technology Security Certification and Accreditation Process (DITSCAP). The former standard DoD process for identifying information security requirements, providing security solutions, and managing IS security activities.

DON Application and Database Management System (DADMS). The database managed by the DON and the Functional Area Managers (FAM) designed as a repository to store, track and approve applications, databases, systems, and networks for operation with in the DON.

Enclave. Collection of computing environments connected by one or more internal networks under the control of a single approval authority and security policy, including personnel and physical security. Enclaves always assume the highest MAC and security classification of the AIS applications or outsourced IT-based processes they support, and derive their security needs from those systems. They provide standard IA capabilities such as boundary defense, incident detection and response, and key management, and also deliver common applications such as office automation and electronic mail. Enclaves are analogous to general support systems as defined in OMB A-130. Enclaves may be specific to an organization or a mission, and the computing environments may be organized by physical proximity or by function independent of location. Examples of enclaves include local area networks and the applications they host, backbone networks, and data processing centers.

Outsourced IT-Based Process. For DoD IA purposes, an outsourced IT-based process is a general term used to refer to outsourced business processes supported by private sector ISs, outsourced information technologies, or outsourced information services. An outsourced IT-based process performs clearly defined functions for which there are readily identifiable security considerations and needs that are addressed in both acquisition and operations.

Platform IT Interconnection. For DoD IA purposes, platform IT interconnection refers to network access to platform IT. Platform IT interconnection has readily identifiable security considerations and needs that must be addressed in both acquisition, and operations. Examples of platform IT interconnections that impose security considerations include remote administration and remote upgrade or reconfiguration. Also see Platform IT.

Enterprise Information Environment (EIE). The common, integrated computing and communications environment of the GIG. The GIG EIE is composed of assets that operate as or that assure local area networks, campus area networks, tactical networks, operational area networks, metropolitan area networks, and wide area networks. The GIG EIE is also composed of assets that operate as or in direct support of end user devices, workstations, and servers that provide local, organizational, regional, or global computing capabilities. The GIG EIE includes all software associated with the operation of EIE assets and the development environments and user productivity tools used in the GIG. The GIG EIE includes a common set of Enterprise and mission specific services, called GIG Enterprise Services, which provide awareness of, access to, and delivery of information on the GIG. DoDI 8115.01 See REFERENCES (k).

Federal Information Security Management Act (FISMA). The FISMA requires Federal departments and agencies develop and implement an organization-wide information security program designed to safeguard IT assets and data. It lays out the Federal framework for annual IT security reviews, reporting, and remediation planning; and it requires that Federal departments and agencies evaluate their information system security programs and report the results on an annual basis. Under FISMA, the term 'information security' means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, which means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity; confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and availability, which means ensuring timely and reliable access to and use of information. See REFERENCES (a).

Global Information Grid (GIG). The globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services, and other associated services necessary to achieve Information Superiority. It also includes National Security Systems as defined in section 5142 of the Clinger-Cohen Act of 1996 See REFERENCES (vv). The GIG supports all DoD, national security, and related intelligence community missions and functions (strategic, operational, tactical, and business), in war and in peace. The GIG provides capabilities from all operating locations (bases, posts, camps, stations, facilities, mobile platforms, and deployed sites). The GIG provides interfaces to coalition, allied, and non-DoD users and systems. DoDD 8100.1 See REFERENCES (d).

Includes any system, equipment, software, or service that meets one or more of the following criteria:

Transmits information to, receives information from, routes information among, or interchanges information among other equipment, software, and services.

Provides retention, organization, visualization, IA, or disposition of data, information, and/or knowledge received from or transmitted to other equipment, software, and services.

Processes data or information for use by other equipment, software, or services.

Non-GIG IT is stand-alone, self-contained, or embedded IT that is not and will not be connected to the enterprise network.

DoD Information Technology Security Certification and Accreditation Process (DITSCAP). The standard DoD process for identifying information security requirements, providing security solutions, and managing IS security activities.

Environment. Aggregate of external procedures, conditions, and objects effecting the development, operation, and maintenance of an IS.

IA Capabilities and Services. Information technology (hardware, software, and firmware), data, facilities, and human activities designed and implemented to provide integrity, confidentiality, non-repudiation, identification and authentication, and availability of DoD ISs through the exercise of management, operational, technical, and personnel controls.

IA Component of the GIG. The collective and interdependent IA capabilities and services of the ISs that comprise the GIG.

IA Component of the GIG Architecture. An abstract expression of current and future instances of the IA Component of the GIG.

IA Component of the System Architecture. An abstract expression of all current or future IA/security technical solutions employed within a DoD IS and all interfaces to core enterprise or COI services for IA/security. The IA/security architecture assigns and portrays the assigned IA roles and behavior of all inherent IA/security features and functions and all embedded IA or IA-enabled IT products, and prescribes rules for interaction and interconnection. The IA component of the system architecture must conform to the IA Component of the GIG Architecture.

IA Control. An objective IA condition of integrity, availability, or confidentiality achieved through the application of specific safeguards or through the regulation of specific activities that is expressed in a specified format (i.e., a control number, a control name, control text, and a control class). Specific management, personnel, operational, and technical controls are applied to each DoD IS to achieve an appropriate level of integrity, availability, and confidentiality in accordance with DoDI 8500.2. See REFERENCES (e).

IA Control Set. Collection of IACs associated with a level of integrity, availability, and confidentiality.

Impact Code. Indicates the DoD assessment of the likelihood that a failed IA Control will have IA consequences that have system-wide consequences. It is an indicator of the impact associated with noncompliance or exploitation of the IA Control. May also indicate the urgency with which corrective action should be taken. Impact codes are expressed as High, Medium, Low, where High is the indicator of greatest impact or urgency.

High-Impact Code. The absence or incorrect implementation of this IAC may result in the loss of information resources, unauthorized disclosure of information, or failure to maintain information integrity. Such exploitation may severely disrupt or impede GIG situational awareness, management, and control; system operations; or user access.

Medium-Impact Code. The absence or incorrect implementation of this IAC may moderately disrupt or impede GIG situational awareness, management, and control; system operations; or user access.

Low-Impact Code. The absence or incorrect implementation of this IAC may minimally disrupt or impede GIG situational awareness, management, and control; system operations; or user access.

Implementation Procedures. Describes the required steps and provides guidance for implementing DoD IACs.

Information Assurance (IA). Measures that protect and defend information and ISs by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of ISs by incorporating protection, detection, and reaction capabilities.

Information Assurance Manager (IAM). Individual responsible for a program, organization, system, or enclave's information assurance program. While the term IAM is favored within the DoD, it may be used interchangeably with the title Information Systems Security Manager (ISSM).

Information Assurance Officer (IAO). An individual responsible to the IAM for ensuring that the appropriate operational IA posture is maintained for a DoD IS or organization. DoDI 8500.2. See REFERENCES (e).

Information Assurance Tracking System (IATS). The Navy C&A repository, process and tracking tool.

Information Category. The term used to bound information and tie it to an information security policy.

Information Owner. Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.

Information Resources. Information and related resources, such as personnel, equipment, funds, and information technology. DoDD 8000.1. See REFERENCES (ww).

Information Security Policy. The aggregate of public law, directives, regulations, rules, and practices that prescribe how an organization manages, protects, and distributes information.

Information System. Set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display or transmission of information. Any telecommunication or computer-related equipment or interconnected system or subsystems of equipment that is used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of voice and/or data, and includes software, firmware, and hardware.

Information Systems Security Engineering/Engineer (ISSE). A process (or the person performing the process) that captures and refines information protection requirements and ensures their integration into IT acquisition processes through purposeful security design or configuration.

Information Technology (IT). The hardware, firmware, and software used as part of the IS to perform DoD information functions. This definition includes computers, telecommunications, automated ISs, and automatic data processing equipment. IT includes any assembly of computer hardware, software, and/or firmware configured to collect, create, communicate, compute, disseminate, process, store, and/or control data or information.

Information Technology Security (ITSEC). Protection of information technology against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats. Protection and maintenance of confidentiality, integrity, availability, and accountability.

Infrastructure-Centric. A security management approach that considers ISs and their computing environment as a single entity.

Inheritance. Inheritance in the context of DIACAP refers to the state in which an IA Control along with the control validation results and compliance status is shared across two or more systems for the purposes of C&A. Through inheritance, an existing IA Control and its C&A status, would extend from an “originating” system to another “receiving” system in order to model a real-word scenario of shared security infrastructure or capability. Inheritance is intended to reduce the complexity of testing by allowing the unilateral application of validation test results to all systems sharing the security capability. The DIACAP Implementation Plan specifically identifies IACs inherited between systems.

Integrator. An organization or individual that unites, combines, or otherwise incorporates IS components with another system(s).

Integrity. Quality of an IS reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. Note that, in a formal security mode, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information.

Interim Authorization to Operate (IATO). Temporary authorization granted by a DAA for a IS to process information based on preliminary results of a security evaluation of a system.

Interim Authorization to Test (IATT). Temporary authorization to test an IS in a specified operational information environment within the timeframe and under the conditions or constraints enumerated in the written authorization.

Metropolitan Area Network (MAN). A MAN is a computer network covering a large military geographic area, like a grouping of posts, stations, or bases.
A network that uses routers and public communications links for a specific metropolitan area (e.g., a city) respectively. The defining characteristics of MANs, in contrast to wide-area networks (WANs), include their smaller geographic range.

Mission Area (MA). A defined area of responsibility whose functions and processes contribute to accomplishment of the mission. Those mission areas are: The Warfighting Mission Area (WMA), Business Mission Area, (BMA), Defense Intelligence Mission Area (DIMA), and Enterprise Information Environment Mission Area (EIEMA), DoDD 8115.01.

Mission Assurance Category (MAC). Applicable to DoD ISs, the mission assurance category reflects the importance of information relative to the achievement of DoD goals and objectives, particularly the war fighters' combat mission. Mission assurance categories are primarily used to determine the requirements for availability and integrity. The DoD has three defined mission assurance categories.

Mission Assurance Category I (MAC I). 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 of a MAC I system are unacceptable and could include the immediate and sustained loss of mission effectiveness. MAC I systems require the most stringent protection measures.

Mission Assurance Category II (MAC II). Systems handling information that is important to the support of deployed and contingency forces. The consequences of loss of integrity are unacceptable. Loss of availability is 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.

Mission Assurance Category III (MAC III). Systems handling information that is necessary for conducting day-to-day business, but does not materially affect support to deployed or contingency forces in the short term. The 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.

Net-Centricity. Net-Centricity is a robust, globally connected network environment (including infrastructure, systems, processes, and people) in which data is shared quickly and seamlessly among users, applications, and platforms. Net-centricity enables substantially improved military situational awareness and significantly shortened decision making cycles. Net-centric capabilities enable network-centric operations and Net-Centric Warfare (NCW).

Outsourced IT-based process. For DoD IA purposes, an outsourced IT-based process is a general term used to refer to outsourced business processes supported by private sector ISs, outsourced information technologies, or outsourced information services. An outsourced IT-based process performs clearly defined functions for which there are readily identifiable security considerations and needs that are addressed in both acquisition and operations.

Platform IT. Platform IT refers to 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; DoDI 8500.2.

Platform IT Interconnection. For DoD IA purposes, platform IT interconnection refers to network access to platform IT. Platform IT interconnection has readily identifiable security considerations and needs that must be addressed in both acquisition, and operations. Examples of platform IT interconnections that impose security considerations include remote administration and remote upgrade or reconfiguration. Also see Platform IT.

Information Technology (IT) Security Plan of Action and Milestones (POA&M). A plan of action and milestones required for any accreditation decision that requires corrective actions. The POA&M addresses: (1) why the system needs to operate; (2) any operational restrictions imposed to lessen the risk during the interim authorization; (3) specific corrective actions necessary to demonstrate that assigned IA Controls have been implemented correctly and are effective; (4) the agreed upon timeline for completing and validating corrective actions; and (5) the resources necessary and available to properly complete the corrective actions.

Principal Accrediting Authority (PAA). The senior official having the authority and responsibility for ISs within a GIG Mission Area.

Process. The actions/tasks accomplished by the people responsible for the creation, review, certification and accreditation of a C&A package according to the DIACAP rule-set.

Program or System Manager (PM or SM). Official responsible for the overall procurement, development, early and seamless integration, IA, modification, or operation and maintenance of an assigned DON IS throughout the system life cycle.

Residual Risk. Portion of risk remaining after security measures have been applied.

Risk. Possibility that a particular threat will adversely impact an IS by exploiting a particular vulnerability.

Risk Assessment. Process of analyzing threats to and vulnerabilities of an IS, and the potential impact resulting from the loss of information or capabilities of a system. This analysis is used as a basis for identifying appropriate and cost effect security countermeasures.

Risk Management. Process of managing risks to agency operations (including mission, function, image, or reputation), agency assets or individuals resulting from the operation of an information system. It includes risk assessment; cost-benefit analysis; the selection, implementation and assessment of security controls; and the formal authorization to operate the system. The process considers effectiveness, efficiency and constraints due to laws, directives, policies, or regulations.

Security. Measures and controls that ensure confidentiality, integrity, availability, and accountability of the information processed and stored by a computer.

Security Inspection. Examination of an IS to determine compliance with security policy, procedures, and practices.

Security Process. The activities that monitor, evaluate, test, certify, accredit, and maintain the system accreditation throughout the system life-cycle.

Security Requirements. Types and levels of protection necessary for equipment, data, information, applications, and facilities to meet IS security policy.

Security Relevant Event. An event that would cause a harmful change in an IS or its environment, or that a competent IAM would consider to require noting, investigation, or prevention (e.g., the discovery of malicious code in an IS, the discovery of an attempt to connect an unapproved device to the network).

Senior Information Assurance Officer (SIAO). Official responsible for directing an organization IA program on behalf of the organization CIO.

Security Test and Evaluation (ST&E). Examination and analysis of the safeguards required to protect an IT system, as they have been applied in an operational environment, to determine the security posture of that system.

Sensitive Information. Information the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conducting of federal programs, or the privacy to which individuals are entitled under 5 U.S.C. Section 552a (the Privacy Act), but that has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

Severity Code. Indicates the CA's assessment of the likelihood of system-wide IA consequences, given a single or multiple findings. It is the Code assigned to a system IA security weakness by a CA as part of a certification analysis to indicate (1) the risk level associated with the IA security weakness and (2) the urgency with which the corrective action must be completed. Severity codes are expressed as "CAT I, CAT II, CAT III," where CAT I is the indicator of greatest risk and urgency.

CAT I Severity Code. Assigned to findings that allow primary security protections to be bypassed, allowing immediate access by unauthorized personnel or unauthorized assumption of super-user privileges, and that usually cannot be mitigated.

CAT II Severity Code. Assigned to findings that have a potential to lead to unauthorized system access or activity. CAT II findings can usually be mitigated and will not prevent an ATO from being granted.

CAT III Severity Code. Assigned to recommendations that will improve IA posture but are not required for an authorization to operate.

Site. One or more information systems under the control of a single IAM are termed a site. A site may include more than one facility or location (e.g., building, campus or base) provided those locations under the purview of the IAM. A site consists of one or more security domains. Sites may have additional security domains containing other classifications, coalition partner information. Each security domain contains one or more enclaves. An enclave is a collection of computing environments connected by one or more internal networks. A security domain is a logical grouping of systems based on security policy. An enclave is a grouping of systems based on a physical characteristic such as location or connectivity. Enclaves are characterized by their membership in a security domain. This membership may be temporal in the case of periods processing.

Site Accreditation. The accreditation of one or more information systems under the control of an IAM and operational DAA as a single accreditation is termed site accreditation. Site accreditation combines the system specific information from C&A packages developed under DoD IA C&A policies into an integrated IA document describing that site and the security controls common to the domains at that site.

System. A set of interrelated components consisting of mission, environment, and architecture as a whole.

System Owner. A System Owner (SO) is any entity who has the responsibility to develop and field a IS within the DON. In IA the SO has the same role, responsibilities and requirements as a PM.

Stand-Alone Information System. An IS operating independently of any other IS within an environment physically secured commensurate with the highest classification of material processed or stored thereon. DoDI 8580.1 See REFERENCES (ii).

System Identification Profile (SIP). An information base, i.e., a document, collection of documents, or collection of data objects within an automated IS that uniquely identifies an IS within the DIACAP and contains established management indicators, e.g., DIACAP status.

System Integrity. Quality of an IT system to perform its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

Threat. Any circumstance or event with the potential to adversely impact an IS through unauthorized access, destruction, disclosure, modification of data, and/or denial of service.

Threat Assessment. Formal description and evaluation of threat to an IS.

User. Individual or process authorized to access an IS.

User Representative (UR). Individual or organization that represents the user community in the DIACAP.

Validation. Activity applied throughout the system life cycle, to confirm or establish by testing, evaluation, examination, investigation, or competent evidence that an IS's assigned IACs are implemented correctly and are effective in their application.

Validation Event. The execution of one or more Validation Procedures for an IS.

Validation Procedure. Describes the requisite preparatory steps and conditions, actual validation steps, expected results, and criteria and protocols for recording actual results, and may include associated supporting background material, sample results, or links to automated testing tools.

Validator. Entity responsible for conducting a validation procedure.

Verification. The process of determining compliance of the evolving IT system specification, design, or code with the security requirements and approach agreed on by the users, acquisition authority, and the DAA.

Vulnerability. Weakness in an IS, system security procedures, internal controls, or implementation that could be exploited.

Vulnerability Assessment. Systematic examination of an IS or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation

Wide Area Network (WAN). A computer network that covers a broad area (i.e., any network whose communications links cross metropolitan, regional, or national boundaries. The largest and most well-known DoD example of a WAN is the NIPRNET.

ENCLOSURE (3) ACRONYMS

ACRONYM	DEFINITION
ACAT	Acquisition Category
ASD(NII)	Assistant Secretary of Defense for Networks and Information Integration
AIS	Automated Information System
ATD	Authorization Termination Date
ATO	Authorization to Operate
BMA	Business Mission Area
C&A	Certification and Accreditation
C/NC	Compliant/Non-Compliant
CA	Certifying Authority
CAR	Certifying Authority Representative
CAT	Category
CCM	Configuration Control and Management
CDS	Cross-Domain Solution
CDD	Capabilities Development Document
CDR	Critical Design Review
CFO	Chief Financial Officer
CIO	Chief Information Officer
CJCS	Chairman Joint Chiefs of Staff
CJCSI	CJCS Instruction
CJCSM	CJCS Manual
CL	Confidentiality Level
CM	Configuration Management
CMC	Commandant of the Marine Corps
CMP	Centrally Managed Program
CNO	Chief of Naval Operations
CO	Commanding Officer
COCO	Commercially Owned Commercially Operated
COGO	Commercially Owned Government Operated
CONOPS	Concept of Operations
COOP	Continuity of Operations Plan
COI	Communities of Interest
COTS	Commercial Off-The-Shelf
CPD	Capabilities Production Document
DAA	Designated Accrediting Authority
DADMS	DON Application Database Management System
DATO	Denial of Authorization to Operate
DCI	Director Central Intelligence
DCID	Director Central Intelligence Directive
DCNO	Deputy Chief of Naval Operations
DDAA	Developmental Designated Accrediting Authority
DIACAP	DoD Information Assurance Certification and Accreditation Process
DIAM	Defense Intelligence Agency Manual

ACRONYM	DEFINITION
DIMA	Defense Intelligence Mission Area
DIP	DIACAP Implementation Plan
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DITPR-DON	DoD Information Technology Portfolio Repository – Department of the Navy
DITSCAP	DoD Information Technology Security Certification and Accreditation Process
DLA	Defense Logistics Agency
DNI	Director of National Intelligence
DoD	Department of Defense
DoDD	DoD Directive
DoDI	DoD Instruction
DoDIIS	DoD Intelligence Information System
DON	Department of the Navy
DREN	Defense Research and Engineering Network
DRR	Design Readiness Review
E.O.	Executive Order
EIE	Enterprise Information Environment
EIEMA	Enterprise Information Environment Mission Area
FAM	Functional Area Manager
FCA/SVR	Functional Configuration Audit/Service Verification Review
FDM	Functional Data Manager
FISMA	Federal Information Security Management Act
FRP	Full Rate Production
GAO	Government Accountability Office
GCCS	Global Command and Control System
GIG	Global Information Grid
GOCO	Government Owned Commercially Operated
GOGO	Government Owned Government Operated
GOTS	Government Off-The-Shelf
HQMC	Headquarters Marine Corps
IA	Information Assurance
IAC	Information Assurance Control
IAM	Information Assurance Manager
IAO	Information Assurance Officer
IATO	Interim Authorization to Operate
IATT	Interim Authorization to Test
IAVA	Information Assurance Vulnerability Alert
IAVB	Information Assurance Vulnerability Bulletin
IAVM	Information Assurance Vulnerability Management
IC	Intelligence Community
ICD	Initial Capabilities Document
ID	Identification
IG	Inspector General

ACRONYM	DEFINITION
IM	Information Management
IOT&E	Initial Operational Test & Evaluation
IS	Information System
ISSE	Information Systems Security Engineer/Engineering
ISSM	Information Systems Security Manager
IT	Information Technology
ITS	Information Technology Security
JDCSISSS	Joint DoDIIS Cryptologic SCI Information Systems Security Standard
JCIDS	Joint Capabilities Integration Development System
JIC	Joint Information Center
JWICS	Joint Worldwide Intelligence Communications System
KS	Knowledge Service
LAN	Local Area Network
MA	Mission Area
MAC	Mission Assurance Category
MAIS	Major Automated Information System
MCEN	Marine Corps Enterprise Network
MCTN	Marine Corps Tactical Network
MC	Mission Critical
ME	Mission Essential
MOA	Memorandum of Agreement
MS	Mission Support
MSC	Major Subordinate Commands
MS-A, B or C	[Acquisition] Milestone A, B, or C
NC2-ESI	Nuclear Command and Control Extremely Sensitive Information
NE	Network Environment
NIAP	National information Assurance Partnership
NIPRNET	Non-Classified Internet Protocol Router Network
NIST	National Institute of Standards and Technology
NMCI	Navy Marine Corps Intranet
NNPI	Naval Nuclear Propulsion Information
NOC	Network Operations Center
NSA	National Security Agency
NSTISSP	National Security Telecommunications and Information Security Policy
ODAA	Operational DAA
OIC	Officer-In-Charge
OMB	Office of Management and Budget
OSD	Office of the Secretary of Defense
OSN	Office of the Secretary of the Navy
PAA	Principal Accrediting Authority
PCA	Physical Configuration Audit
PDR	Preliminary Design Review
PII	Personally Identifiable Information
PM or SM	Program or System Manager

ACRONYM	DEFINITION
PMO	Program Management Office
POA&M	Plan of Action and Milestones
POC	Point of Contact
POR	Program of Record
PPBE	Planning, Programming, Budgeting and Execution
PPS	Ports, Protocols and Services
PPSM	Ports, Protocols and Services Management
RDT&E	Research, Development, Test, and Evaluation
RNOSC	Regional Network Operations Security Center
RTM	Requirements Traceability Matrix
SA	Systems Administrator
SCI	Sensitive Compartmented Information
SDLC	Systems Development Life Cycle
SFR	System Functional Review
SIAO	Senior Information Assurance Officer
SIP	System Identification Profile
SIPRNET	Secret Internet Protocol Router Network
SLC	System Life Cycle
SM	System Manager
SO	System Owner
SRR	System Requirements Review
SSR	System Specification Review
ST&E	System Test & Evaluation
STIG	Security Technical Implementation Guide
TAG	Technical Advisory Group
T&E	Test and Evaluation
TRR	Test Readiness Review
UR	User Representative
UTNpp	Unclassified Trusted Network Protect Policy
WMA	Warfighting Mission Area

ENCLOSURE (4) EXAMPLE OF MINIMUM C&A PACKAGE COMPONENTS

The DIACAP C&A Package	
Comprehensive C&A Package Components:	**Enclosure**
• **System Identification Profile (SIP)**	**5**
• **DIACAP Implementation Plan (DIP)**	
C&A Plan	**6**
Mission Description	
CONOPS Summary	
User Description and Clearances	
Operating and Computing Environment	
Physical Security Measures/Facilities	
Threat Analysis	
Security Roles	
System Architecture Diagram	
Accreditation Boundary	
External Interfaces and Data Flow	
Hardware List	
Software List	
Ports, Protocols and Services (PPS)	
C&A Tasks and Milestones	
Contingency Plan	
IAC Implementation Plan	**7**
Validation Plan and Procedures	**8**
DIP Concurrence Sheet	**9**
C&A package Signature Page	**10**
• **DIACAP Scorecard**	**11**
Certification Determination	**12**
Accreditation Decision	**13**
• **POA&M**	**14**
Statement of Compliance	**15**

ENCLOSURE (5) EXAMPLE OF SYSTEM IDENTIFICATION PROFILE (SIP) TEMPLATE

Register System with DoD Component IA Program

System registration establishes the relationship between the DoD IS and the governing DoD Component IA program which continues until the DoD IS is decommissioned. DIACAP registration facilitates organizational IT management and FISMA reporting. It involves recording descriptive system acquisition and IA data in such a manner as to allow unique system identification. Registration commences a dialog between the DoD information system owner and the DoD Component CIO that should continue until the DoD information system is decommissioned.

The set of information gathered during system registration is referred to as the System Identification Profile (SIP), which becomes part of the DIACAP Package for the information system, and is maintained throughout the system's life cycle. The SIP identifies the minimum data requirements, plus explanations, for registering an information system with the Component. An overview of the type of information included in the System Identification Profile can be seen in the table below. Typically, this information can be found in program/project documentation, such as the initial capabilities document, system requirements/specifications, architecture and design documents, etc.

System Identification Profile (SIP) Instructions			
Field ID	**Data Element Descriptor**	**Data Element**	**Required/Conditional**
1	System ID:	<Unique, system generated ID for each individual system - Developed and maintained at ODAA>	Required for ODAA Action Officers.
2	DITPR-DON:	<Number associated with System from DITPR DON Database>	Conditional – required for those systems mandated to be registered in DITPR-DON.
3	DADMS ID:	<Number associated with System from DADMS Database>	Conditional – required for all applications mandated to be register within DADMS.
4	FAM Status (Applications ONLY):	<Select from: Approved, Approved with Interim Waiver (AIW), Approved With Restrictions (AWR), Disapproved, or Not Applicable>	Conditional.
5	CCSD:	<CCSD of the Circuit>	Conditional on whether a circuit is associated with request.
6	**Site Type:**	<Select from NMCI, One-Net, IT-21, or Legacy>	Required.
7	**Site/Command Name:**	<The organization that owns or controls the DoD Information system>	Required.
8	**UIC:**	<Unit Identification Code of site requesting authorization>	Required.

System Identification Profile (SIP) Instructions			
Field ID	**Data Element Descriptor**	**Data Element**	**Required/Conditional**
9	**Echelon II Command:**	<EII that requesting site reports to>	Required.
10	**User/Claimant:**	<User of the system>	Required.
11	**Governing DoD Component IA Program:**	<Navy DAA, Air Force DAA, DDAA, etc.>	Required.
12	**System name:**	<Name that uniquely identifies system>	Required.
13	**System Acronym:**	<System Acronym>	Required.
14	**System Version or Release Number:**	<Version of system identified in ID #12>	Required.
15	**System Description:**	<A narrative description of the system, its function, and uses>	Required.
16	**Reason for Request:**	<Indicate the Reason for the Request>	Required.
17	**Cross Domain Solution (CDS):**	<Is there a Cross Domain Solution associated with system> "CDS consists of any information that crosses a security domain (either manually (sneaker-net) or automated). The reason it is stated this way and not including only classification labels (e.g. NIPR to SIPR) is so that it can include information that is shared with our allies."	Required.
18	**NATO:**	<Will NATO access be required (SIPRNET Only)>	Required.
19	**DIACAP Activity:**	<Initiate and Plan IA C&A Implement, validate Assigned IA Controls, make Certification Determination and Accreditation Decision, maintain ATO and conduct reviews>	Required.
20	**System Life Cycle or Acquisition Phase:**	<1. Concept Refinement 2. Milestone A (MS-A) Technology Development, 3. MS-B System Development and Demonstration 4. MS-C Production and Deployment Demonstration 5. Operations and Support 6. Disposal or Decommissioning>	Required.
21	**Information System Type:**	<Enclave, AIS Application, Outsourced IT-Based Process, Platform IT Interconnection> (reference DoDD 8510.bb for definitions of "DoD Information Systems")	Required.
22	**Mission Assurance Category (MAC):**	<I, II, III>	Required.
23	**Confidentiality Level:**	<Public, Sensitive, Classified>	Required.
24	**Mission Criticality :**	<Mission Critical (MC), Mission Essential (ME), or Mission Support (MS)>	Required.
25	**Accreditation Vehicle:**	<8500.2, (DCID) 6/3>	Required.

System Identification Profile (SIP) Instructions			
Field ID	**Data Element Descriptor**	**Data Element**	**Required/Conditional**
26	Additional Accreditation Vehicles:	<e.g. Privacy Requirements, Special Access Requirements, Cross Domain Solution (CDS) Ticket Number, Non Classified Internet Protocol Router Network (NIPRNET, Secret Internet Protocol Router Network (SIPRNET), or GIG CAP Identifier, Ports, Protocols and Services Management (PPSM) Identifier>	As specified.
27	Certification Date (DD-MMM-YYYY):	<Date approved by DAA>	Conditional if approval has already been granted.
28	**Accreditation Request Type:**	< ATO, IATO, IATB, IATC, or IATT>	Required.
29	If IATO, which iteration:	<Indicate whether this is the initial IATO (1), or an extension of the initial IATO (2, 3, 4, etc.)>	Conditional (Required for all IATOs).
30	Authorization Termination Date (DD-MMM-YYYY):	Insert Authorization Termination Date, which is the date assigned by the DAA to indicate the date upon which accreditation is terminated for an ATO, IATO, or IATT.	Conditional.
31	DIACAP Team Roles, Member Names and Contact Information:	<e.g. PM or SM, IAM, User Representative, CA, DAA, SIAO, CIO>	Required to be filled in at bottom of SIP (CA & DAA hard coded).
32	Acquisition Category (ACAT):	<Categorization of Project/Program relative to ACAT designations> There are two reference policies applicable to this line item: DODI 5000.2 and SECNAVINST 5000.2C. They are different in that the SECNAVINST has more ACAT categories and sub-categories (thus different trigger levels). Visit the following link for a depiction of the differences: http://www.ntsc.navy.mil/resources/library/acqguide/acat.htm	As specified.
33	Type of IT Investment:	<What type of IT investment is this (Business system, Infrastructure, NSS, Initiative, Not Applicable)?>	As specified.
34	Software Category:	<COTS, GOTS or Custom business system>	As specified.
35	**Privacy Impact Assessment:**	<Yes/No> (ref: DON CIO message with DTG R 081547Z FEB 07 "DEPARTMENT OF THE NAVY PRIVACY IMPACT ASSESSMENT (PIA) GUIDANCE")	Required.
36	**E-Authentication Risk Assessment:**	<Yes/No> E-authentication is found on the DITPR-DON E-Authenticate Assessment Questions 1), 2), 3) are Required for ALL Systems. Questions 4) - 29) Required if Question 1) and 2) Answers are 'Yes' and 3) is 'Partially' or 'All'. 1) Browser Based: Yes 2) External Facing: No 3) End User Authentication Required: All	Required.
37	**Annual Security Review Date (DD-MMM-YYYY):**	<What was the date of the annual security review required by FISMA and DoD?>	Required.

System Identification Profile (SIP) Instructions			
Field ID	**Data Element Descriptor**	**Data Element**	**Required/Conditional**
38	System Operation:	<Government (DoD) Owned Government Operated (GOGO), Government (DoD) Owned Commercially Operated (GOCO), Commercially Owned Government (DoD) Operated (COGO), Commercially Owned Commercially Operated (COCO)>	As specified.
39	**Contingency Plan:**	<Contingency Plan Included - Yes/No>	Required.
40	**Contingency Plan Tested:**	<Has the Plan been tested - Yes/No> This field is to be completed in accordance with FISMA requirements for yearly verification of Security/IA controls.	Required.
41	Initial Security Controls Tested Date (DD-MMM-YYYY):	<Indicate the last date system security controls were tested> This field is to be completed in accordance with FISMA requirements for yearly verification of Security/IA controls.	Conditional
42	First Annual Partial Tested Date (DD-MMM-YYYY):	<The date that the first partial test was conducted for an ATO system> This field is to be completed in accordance with FISMA requirements for yearly verification of Security/IA controls.	Conditional - if the Initial has already been performed
43	Second Annual Partial Tested Date (DD-MMM-YYYY):	<The date that the second partial test was conducted for an ATO system> This field is to be completed in accordance with FISMA requirements for yearly verification of Security/IA controls.	Conditional on whether the initial and first tests have been performed.
44	Compliant with all Federal, DoD, and DON IA policies: (DoDD 8500.1, DoDI 8500.2, DoD 8510.1-M, IAVM Compliance, DoD IA Policies, DISN Connection Approval Policies, DON IA Policies, DON UTNpp, DoD/DON PKI Policies, DoD/DON Wireless Policies)	<Replaces the need for the IA Compliance Letter, System Owner must ensure that they are compliant with all mentioned Directives, Instructions, and Policies before making a selection for this option>	Required.
45	Systems installed in a Server Farm are operated IAW Their Type of Accreditation	<Yes/No> Systems installed within a Server Farm must be operated IAW their Type Accreditation.	Conditional.

System Identification Profile (SIP) Instructions			
Field ID	**Data Element Descriptor**	**Data Element**	**Required/Conditional**
46	Registration of Ports with DoD Ports, Protocols, and Services (PPS) (if applicable):	<This is for registering ports with the DoD Internet Access Points (IAPs) to include in the DoD routes outside of the Navy Enclave - Navy POC for PPS Registration is: CWO3 Santos (NETWARCOM N51) (757) 417-6754 ext 0 DSN 537 carlos.m.santos@navy.mil / carlos.m.santos@navy.smil.mil (http://iase.disa.smil.mil/ports)>	Conditional.
47	**Impact Statement**	<Compelling Impact statement if the sys/net/app is not accredited by the Impact Date>	Required.
48	**Impact Date**	<Date in which Impact will occur>	Required.

Sample SIP provided below:

System Identification Profile

Site/Command Name		**System Name**	**System Acronym**	**Version**	**DITPR-DON ID#**
0		**0**	**0**	**0**	**0**
1	System ID:		***For ODAA Use Only***		
2	DITPR-DON (ITSRD ID) #:				
3	DADMS ID#:				
4	FAM Status:				
5	CCSD:				
6	**Site Type:**				
7	**Site/Command Name:**				
8	**UIC:**				
9	**Echelon II Command:**				
10	**User/Claimant:**				
11	**Governing DoD Component IA Program:**		Navy DAA		
12	**System name:**				
13	**System Acronym:**				
14	**System Version or Release Number:**				
15	**System Description:**				
16	**Reason for Request:**				
17	**Cross Domain Solution (CDS):**				
18	**NATO:**				
19	**DIACAP Activity:**				
20	**System Life Cycle or Acquisition Phase:**				
21	**Information System Type:**				
22	**MAC:**				
23	**Confidentiality Level:**			(Please list special handling requirements)	

24	**Mission Criticality :**	
25	**Accreditation Vehicle:**	
26	Additional Accreditation Vehicles:	
27	Certification Date (DD-MMM-YYYY):	
28	**Accreditation Request Type:**	
29	If IATO, which iteration:	
30	Authorization Termination Date (DD-MMM-YYYY):	
31	DIACAP Team Roles, Member Names and Contact Info:	**See Table Below.**
32	Acquisition Category (ACAT):	
33	Type of IT Investment:	
34	Software Category:	
35	**Privacy Impact Assessment:**	
36	**E-Authentication Risk Assessment:**	
37	**Annual Security Review Date (DD-MMM-YYYY):**	
38	System Operation:	
39	**Contingency Plan:**	
40	**Contingency Plan Tested:**	
41	Initial Security Controls Tested Date (DD-MMM-YYYY):	
42	First Annual Partial Tested Date (DD-MMM-YYYY):	
43	Second Annual Partial Tested Date (DD-MMM-YYYY):	
44	**Compliant with all Federal, DoD, and DON IA policies: (DoDD 8500.1, DoDI 8500.2, DoD 8510.1-M, IAVM Compliance, DoD IA Policies, DISN Connection Approval Policies, DON IA Policies, DON UTNpp, DoD/DON PKI Policies, DoD/DON Wireless Policies)**	
45	Systems installed in a Server Farm are operated IAW Their Type of Accreditation:	
46	Registration of Ports with DoD Ports, Protocols, and Services (PPS) (if applicable):	

47	**Impact Statement:**	
48	**Impact Date (DD-MMM-YYYY):**	

DIACAP Team Roles, Member Names and Contact Information			
	Full Name	**Phone**	**Email**
Navy Certifying Authority (CA):	Skip Thaeler	858-537-8863	navy_ca@navy.mil
Certification Agent:			
CIO:			
Navy ODAA:	Richard Voter	757-417-6719 ext 0	nnwc_odaa@navy.mil
Echelon II POC:			
IAM:			
PM/SM:			
DDAA (Developmental DAA):			
RDAA (RDT&E DAA):			
User Representative:			

Mandatory Fields are in BOLD

ENCLOSURE (6) EXAMPLE OF C&A PLAN

Note: ***The following document titles are not templates, but are required elements of the C&A Plan. These elements should be created and uploaded or attached as separate supporting artifacts:***

MISSION DESCRIPTION:
Explain the overall mission of the system and the assigned duties to be performed by each resource.

CONCEPT OF OPERATIONS (CONOPS) SUMMARY:
Develop a summary Concept of Operations (CONOPS). Explain the basic functioning of the system, users, and constraints. Constraints should include restrictions on hours used, personnel to operate the system, hardware limitations, and/or facility requirements.

PHYSICAL SECURITY MEASURES/FACILITIES:
Explain the physical security measures that are required or are in place at the facilities where the system will be installed. Include a description of the physical protections required for the facility housing the system. Identify the procedures needed to counter potential threats that may come from inside or outside the organization. Provide information about physical security and the routine security practices which ensure that unauthorized access to protected resources is prohibited.

EXAMPLE:

> *"The <Command Name> servers reside in Naval Station San Diego room 1234. The Naval Station is protected by a 24-hour Base Police/Shore Patrol roving patrol. The room has a single door with an X08 combination lock and a building enabled with card swipe for access. <Command Name> controls the access list to the room. Person granted access to the room must have a minimum of SECRET clearance and a valid reason to be in the room. The building and room are alarmed and protected by OPNAV security and Base Police/Shore Patrol."*

THREAT ANALYSIS:
Provide a detailed analysis of the present threats to the system. For Type Accreditation, these are the general threats to the system wherever it may be installed (multiple locations). For System and Site Accreditation, these are the specific threats to the system where it is installed (single location). Include a table summarizing threats that are internal and external to the system and explain countermeasures that mitigate or eliminate known threats.

SYSTEM ARCHITECTURE (DIAGRAM):
Provide a diagram of the system that shows the devices, IP ranges, servers, routers, firewalls, etc., that comprise the system (ensure that this diagram is appropriately classified). This image should show other systems or components to which the system is connected for clarity.

ACCREDITATION BOUNDARY (DIAGRAM):
Provide a diagram of the system that shows the accreditation boundary, depicted as a dashed line around those components that are being accredited. This image should show other systems or components to which the system is connected for clarity.

EXTERNAL INTERFACES DATA FLOW (DIAGRAM):
Provide a diagram with an explanation of each external interface, including the classification of the data, the protocol used, the direction (inbound, outbound, or both), and the requirement for cross-domain solutions, etc. An external interface is any data path between a point within the accreditation boundary and a point outside the accreditation boundary. Cross-domain solutions require additional documentation. Note the direction of data flows within the boundary. Classification of the data must be depicted. The IP addresses are only required for the communications that need to be compliant with the UTNpp.

CONTINGENCY PLAN:
Per DON Contingency Plan Message 291600ZFEB, provide a Contingency Plan that does the following:

- Describes the interim measures used to recover and restore the IS following an emergency or system disruption.
- Provides specific guidance to the site IAM on the system requirements for recovery from a disruptive event or emergency that can be incorporated into the site's contingency and COOP plans.
- Contingency Plans shall be exercised at least twice every 12 months for MAC I systems, and at least every 12 months for MAC II and MAC III systems.

These plans will be developed and reviewed for compliance with NIST Computer Security Special Publication 800-34: Contingency Planning Guide for Information Technology Systems, the DOD 8500.2, and corresponding IA controls designated by the system's MAC and confidentiality level.

Note: ***The following documents are templates and required elements of the C&A Plan. These elements should be created from the templates downloadable from the following link:*** https://www.fleetforces.navy.mil/netwarcom/navycanda/default.aspx ***and the completed document uploaded or attached to the C&A Plan as separate supporting artifacts after they are completed:***

USER DESCRIPTION AND CLEARANCES:
Enter a description of users of the system. Include whether any are foreign nationals (if so, from what country or countries) and any special security clearance requirements. Using the table as a template, describe each user type by title and qualifications (clearances, job duties, etc.). Estimate the number of users that the system will support for each user type. If the user type is assigned to foreign national(s), note which country or countries will have this type of access.
See sample template below:

USER DESCRIPTION AND CLEARANCES:				
User Type	**Description: Qualifications**	**Estimated Number of Users**	**Foreign National? (Y/N)**	**Country**

SECURITY ROLES:
Explain the various security roles of the different kinds of users of the system, such as System Administrator, General User, Guest, etc. Identify the security clearance required for each role.

See sample template below:

SECURITY ROLES:		
User Type / Title	**Description of Security Role**	**Required Clearance Level**

HARDWARE LIST:
For Type Accreditation, list the type and model of hardware that makes up the system. For every hardware item, identify whether it is an IA device or IA-enabled device and the Common Criteria evaluation status of the device. For System and Site Accreditation, provide the above with specific identification of the hardware.

See sample template below:

HARDWARE LIST:						
Reference	**Manufacturer**	**IA Enabled (Yes/No)**	**CC Eval Status**	**Device Name**	**Model Number**	**Firmware**

SOFTWARE LIST:
List the kind and version number of the software that makes up the system.
For every software item, identify whether it is IA or IA-enabled and the Common Criteria evaluation status if IA or IA-enabled.

See sample template below:

SOFTWARE LIST:

Application	Version	Purpose	IA Enabled (Yes/No)	CC Eval Status	FAM Status	DADMS #

PORTS, PROTOCOLS AND SERVICES (PPS):
Provide a list of the ports, protocols, and services used by the external interfaces of the system. Indicate the compliance of the system with respect to the Navy-Marine Corps Intranet Trusted Network Protection Policy (UTNPp).

See sample template below:

PORTS, PROTOCOLS, AND SERVICES:

Reference	Description/ Service	Direction - Inbound/ Outbound/ Both	Classification	Port	Protocol	UTNPp Compliant?	Service Host Name

C&A TASKS & MILESTONES:
Provide the C&A plan, including milestones (dates) when major events are expected to occur, such as submission for IATO to the CA, granting of ATO by the DAA, etc. Describe C&A tasks and milestones. Include estimated duration, responsible entity, and completion criteria. Identify, at a high level, the minimum schedule of security activities and other events that will lead to the certification and accreditation of the system.
See sample template below:

C&A TASKS AND MILESTONES:

C&A Activity		Responsible Entity	Completion Criteria	Estimated Start Date	Estimated End Date
1.0 Concept Development / Pre-Systems Acquisition					
	Develop System Concept and Plans				
	Document Mission Description				
	Write CONOPS Summary				
	Document User Description and Clearances				
	Document Operating and Computing Environment				
	Document Physical Security Measures/Facilities				
	Document Threat Analysis Results				
	Document Security Roles				
	Document System-specific Acronyms				
	Document System-specific Definitions				
	Develop DIP C&A Plan				
	Develop Technical Documentation				
	Create Architecture Diagram				
	Define Accreditation Boundary				
	Develop Hardware List				
	Develop Software List				
	Document External Interfaces and Data Flow				
	Document Ports, Protocols, and Services				
	Develop DIP IAC Implementation Plan				
	Develop DIP Validation Plan & Procedures				
	Begin C&A Process				
	Fill Out Preliminary SIP				
	Gather Preliminary DIP Documentation				
2.0 Systems Acquisition/Development					
	Validation and Testing				

	Develop Validation Plan & Procedures				
	Perform Validation				
	Document Results				
	Document DIP Test Results				
	Document DIP IAC Implementation Recommendation				
	Update DIP				
	Develop Scorecard				
	Document Risk Assessment				
	Finish Compiling the C&A Package				
	Develop POA&M for Non-Compliant IACs (if needed)				
	Update SIP				
	Gather Previous Certification Statements				
	Gather Package Documentation				
	Complete the DIACAP Package Signature Page				
	Certification & Accreditation				
	Respond to Requests for additional information (if needed)				
	Resubmit Package Components (if needed)				
	Receive Accreditation Decision				
3.0 Sustainment					
	Transition to Operations & Maintenance				
	Install the System in its Intended Environment				
	Perform Validation				
	Document Results				
	Operate & Maintain System				
	Monitor System Compliance				
	Update Security Documentation				
	Upgrade System				
	Determine whether Re-Certification is Required				
	Retire and Dispose of System				

ENCLOSURE (7) EXAMPLE OF IAC IMPLEMENTATION PLAN

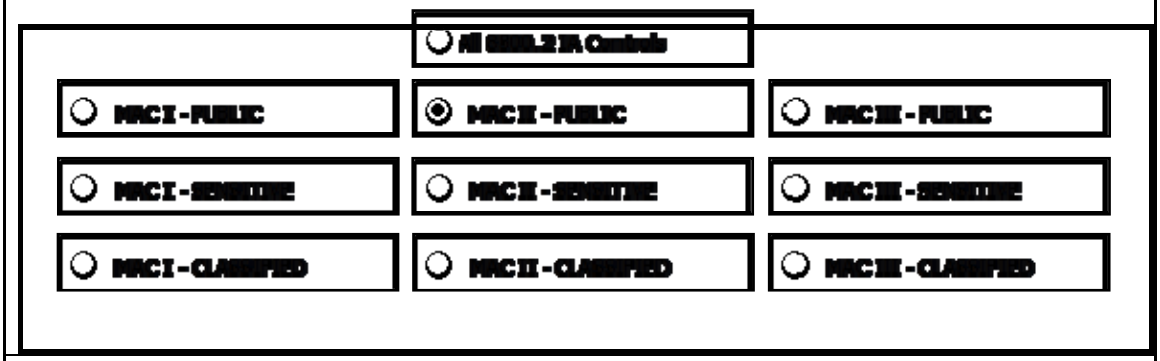
Note: ***The DON IAC Implementation Plan spreadsheet template is downloadable from the following link:*** https://www.fleetforces.navy.mil/netwarcom/navycanda/default.aspx

The IAC Implementation Plan and Guidance template will be generated automatically for Columns 1-6. Columns 7-12 must be filled out to show any Inherited or Non-Applicable IA Controls that have been implemented or are planned. The remaining columns must be filled out by the PM/SO.

See sample template below:

IAC Implementation Plan and Guidance

Select a MAC and CL to generate and view corresponding required IA Controls



Implementation Plan (Columns 1-8)

	1	*2*	*3*	*4*	*5*	*6*	*7*	*8*
	Control Number	**Control Name**	**Subject Area**	**Description**	**Threat/ Vulnerability/ Countermeasure**	**General Implementation Guidance**	**System-Specific Guidance Resource(s)**	**Impact Code**
Row 1								
Row 2								
Row 3								
Row 4								
Row 5								

Implementation Plan (Columns 9-16)

	9	*10*	*11*	*12*	*13*	*14*	*15*	*16*
	Inherited From	**Inheritable**	**Not Applicable Justification**	**Implemented**	**Planned**	**Responsible Entity**	**Resources**	**Estimated Completion Date**
Row 1								
Row 2								
Row 3								
Row 4								
Row 5								

ENCLOSURE (8) EXAMPLE OF VALIDATION PLAN AND PROCEDURES

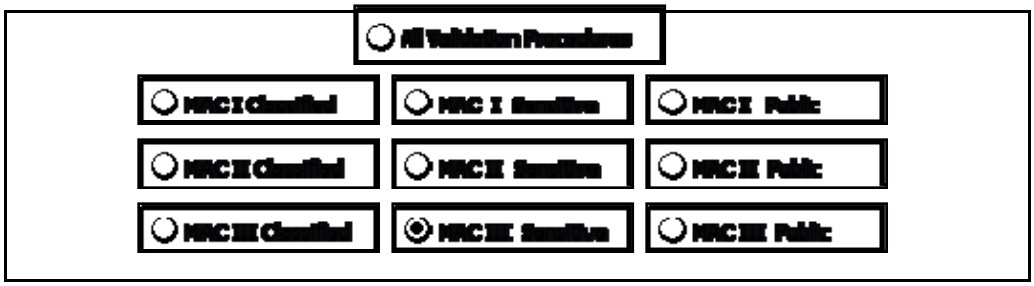
Note: ***The DON Validation Plan and Procedures spreadsheet template is downloadable from the following link:*** https://www.fleetforces.navy.mil/netwarcom/navycanda/default.aspx

The Validation Plan and Procedures template will be generated automatically for Columns 1-7. Columns 8-9 must be filled out to show any Inherited or Non-Applicable IA Controls. The Validation Report Results will be entered into Columns 10-14.

Sample C

Validation Plan & Procedures

Select a MAC Level to generate and view corresponding Validation Plan & Procedures



(Columns 1 - 7) Validation Plan & Procedures

	1 IA Control #	*2* Validation Procedure Number	*3* Procedure Name	*4* Procedure Objective	*5* Procedure Preparation	*6* Procedure Script	*7* Expected Results
Row 1							
Row 2							
Row 3							
Row 4							
Row 5							

(Columns 8 - 14) Validation Results

	8 Inherited From	*9* Not Applicable Justification	*10* Actual Results	*11* Applied Mitigation	*12* CAT	*13* POA&M Recommendation	*14* Risk Analysis
Row 1							
Row 2							
Row 3							
Row 4							
Row 5							

ENCLOSURE (9) EXAMPLE OF DIP CONCURRENCE SHEET TEMPLATE

DON DIACAP Activity 1 Package Concurrence Sheet

Name and Version Number of the System

This DON DIACAP Activity 1 Package documents the security requirements and conditions necessary for Accreditation of *Name and Version Number of the System*. This DIP is a living document that contains or references all information necessary to make an objective, management-level decision and represents an agreement among the *Name of the System* Program Manager (PM), Validator, User Representatives, Certifying Authority (CA), and Designated Accrediting Authority (DAA) on the level of effort, security requirements, and policy required to certify and accredit *Name of the System*.This document addresses certification requirements for a Type Accreditation process as defined in the Department of Defense (DoD) Information Assurance Certification and Accreditation Process (DIACAP). The development of this package is to satisfy DIACAP requirements of the Department of Defense Instruction (DoDI) 8510.01, DoD Information Assurance Certification and Accreditation Process (DIACAP); Federal Information Security Management Act (FISMA); Department of Defense (DoD) Directive (DoDD) 8500.1; DoDI 8500.2; as well as to satisfy the Department of Navy (DON), Chief of Naval Operations (CNO), Information Assurance (IA) Publication (PUB) 5239-13 Volume III. This is a living document and will be updated as the system development progresses and new information becomes available.
The undersigned concur with the information contained in this package and agree that it accurately describes the security implemented for *Name of the System*. This agreement, in effect, certifies that the *Name of the System* meets the security requirements necessary for accreditation, operation up to and including the *[Classification: Unclassified (For Official Use Only) or Secret]* level as described throughout this DIP.

Approved By:

_____ _____

Name Date
Organization
Designated Accrediting Authority (DAA)

_____ _____

Name Date
Organization
Certifying Authority (CA)

_____ _____

Name Date
Organization
Name of the System Program Manager (PM)

_____ _____

Name Date
Organization
Name of the System User Representative

ENCLOSURE (10) EXAMPLE OF C&A PACKAGE SIGNATURE PAGE TEMPLATE

The DIACAP Certification and Accreditation (C&A) Package Signature page shall be drafted and submitted in accordance with current policies and procedures, as approved by each respective Navy or Marine Corps Certifying Authority (CA) and/or Designated Accrediting Authority (DAA). A sample letter has been provided below:

This DIACAP Certification and Accreditation (C&A) Package documents the security requirements and conditions necessary for Accreditation of *Name and Version Number of the System*. This C&A package is a living document that contains or references all information necessary to make an objective, management-level decision and represents an agreement among the *Name of the System* Program Manager (PM), Validator, User Representatives, Certification Authority (CA), and Designated Accrediting Authority (DAA) on the level of effort, security requirements, and policy required to certify and accredit *Name of the System*.

This document addresses certification requirements for a Type Accreditation process as defined in the Department of Defense (DoD) Information Assurance Certification and Accreditation Process (DIACAP). The development of this *Name of the System* C&A package is to satisfy DIACAP requirements of the Department of Defense Instruction (DoDI) Memorandum 8510.bb, Interim Department of Defense (DoD) Information Assurance (IA) Certification and Accreditation (C&A) Process Guidance Memorandum; Federal Information Security Management Act (FISMA); Department of Defense (DoD) Directive (DoDD) 8500.1; DoDI 8500.2; 00 as well as to satisfy the Department of Navy (DON), Chief of Naval Operations (CNO), Information Assurance (IA) Publication (PUB) 5239-13 Volume III. The *Name of the System* C&A package is a living document and will be updated as the system development progresses and new information becomes available.
The undersigned concur with the information contained in this C&A package and agree that it accurately describes the security implemented for *Name of the System*. This agreement, in effect, certifies that the *Name of the System* meets the security requirements necessary for accreditation, operation up to and including the *[Classification: Unclassified (For Official Use Only) or Secret]* level as described throughout this package.

Approved By:

_____

Name Date
Organization
Designated Accrediting Authority (DAA)

_____

Name Date
Organization
Certifying Authority (CA)

_____

Name Date
Organization
Name of the System Program Manager (PM)

_____

Name Date
Organization
Name of the System User Representative

_____

Name Date
Organization
Name of the System User Representative

_____

Name Date
Organization
Name of the System User Representative

_____

Name Date
Organization
Name of the System User Representative

ENCLOSURE (11) EXAMPLE OF DIACAP SCORECARD TEMPLATE

DIACAP Scorecard Template

The DIACAP Scorecard is a summary report that succinctly conveys information on the IA posture of a DoD IS in a format that can be exchanged electronically. It shows the implementation status of an Information System's (IS) assigned IACs (i.e., compliant (C), non compliant (NC), or not applicable (NA)) as well as the C&A status.

Reference	Description
System Name	The name of the system being certified.
System Owner	The organization within the DoD Component that owns, controls, or manages the IS.
IS Type	The IS type (i.e., AIS application, enclave, outsourced IT-based process, and platform IT interconnection). Indicate if the enclave is stand-alone or a DMZ.
DAA	The name and signature of the DAA for the system. Manual or DoD PKI-certified digital signatures are acceptable.

Reference	Description
Accreditation Status	The accreditation decision for the system (i.e., unaccredited, ATO, IATO, IATT, DATO).
Period Covered	Includes the date of the accreditation (if the system has a decision other than unaccredited), and the ATD.
Last Update	The date of the last change that occurred on the scorecard. This is primarily driven by updates to the IA controls and their associated status.
CA	The name of the individual serving as the CA for the system.
Certification Date	The date of the certification.
MAC	The MAC applied to the system.
CL	The CL applied to the system.
IA Control Subject Area	The subject area associated with the IA control.
IA Control Number	The reference number associated with the IA control.
IA Control Name	The name associated with the IA control.
Inherited	An indication (Yes or No) of whether or not the IA control is inherited.
C/NC/NA	An indication of the compliance status of the IA control (i.e., C, NC, NA). An IT Security POA&M is required if NC or NA. Note: NC may indicate either non-implementation or complete failure of the control under testing; it also may indicate a partial failure of a control under testing (e.g., three of four testing points pass).
Impact Code	The impact code associated with the IA control.
Last Update	The date of the last change of the IA control's compliance status (C/NC/NA).

A sample DIACAP Scorecard is shown below:

DIACAP SCORECARD

System Name	System Owner		IS Type
<Insert System Name Here>			
Designated Accrediting Authority (DAA)	Accreditation Status	Period Covered Accreditation Date ATD	Last Update
Certifying Authority (CA)	Certification Date	Mission Assurance Category (MAC)	Confidentiality Level (CL)

■ MAC I, Classified ☐ MAC II, Classified ☐ MAC III, Classified
Classified
☐ MAC I, Sensitive ☐ MAC II, Sensitive ☐ MAC III, Sensitive
☐ MAC I, Public ☐ MAC II, Public ☐ MAC III, Public

IA Control Subject Area	IA Control Number	IA Control Name	Inherited?	C/NC/NA	Impact Code	Last Update

ENCLOSURE (12) EXAMPLE OF ACCREDITATION DECISION

Each Accreditation Decision Letter shall be drafted and submitted in accordance with current policies and procedures, as approved by each respective Navy or Marine Corps Certifying Authority (CA) and/or Designated Accrediting Authority (DAA). A sample letter (Marine Corps Specific) has been provided below:

DEPARTMENT OF THE NAVY
<COMMAND/ORGANIZATION NAME>

<ADDRESS>

IN REPLY REFER TO:
5239
C4/IA
12 Dec 07

From: Designated Accrediting Authority (DAA), Headquarters United States Marine Corps (HQMC), Command, Control, Communications and Computers (C4)
To: Program Manager, Host Based Security System, Marine Corps Network Operations and Security Center

Subj: AUTHORITY TO CONNECT (ATC) THE HOST BASED SECURITY SYSTEM (HBSS) VERSION 3.6.X.X TO THE MARINE CORPS ENTERPRISE NETWORK (MCEN) UNCLASSIFIED BUT SENSITIVE IP ROUTER NETWORK (NIPRNET)

Ref: (a) DoD 8510.1-M, "Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP) Application Manual," 31 Jul 00
(b) Certifying Authority Representative(CAR) letter MCNOSC 5230, 12 Dec 07
(c) DoDI 5200.40, Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP) of 30 Dec 97
(d) CJCSI 6211.02B, Defense Information System Network (DISN): Policy, Responsibilities and Processes of 31 Jul 03
(e) CJCSM 6510.01, Defense-In-Depth: Information Assurance (IA) and Computer Network Defense (CND) of 25 Mar 03 W CH1
(f) DoDI 8500.2 Information Assurance (IA) Implementation of 6 Feb 03
(g) Application Security Plan (ASP) for HBSS of 16 Oct 07
(h) HBSS engineering summary of 12 Oct 07

1. By authority granted in reference (a), an ATC is hereby granted for the connection of HBSS on the MCEN NIPRNET. This ATC is granted based on the information provided in reference (b), in compliance with references (c) through (f), and based on review of the information contained in references (g) through (h).

2. This ATC expires on 15 October 2008, or until there are significant modifications to the system or application in question which essentially alter or may impact the security or architecture as previously accredited (i.e. major version upgrades), events that alter the security posture, or accreditation status of the application, system, or network (i.e. that change the security posture or accreditation status of the overall network. Changes must be submitted in writing through the MCEN CAR for review and

approval by the Marine Corps DAA prior to implementation. Change proposal packages must, at a minimum, include updated topology diagrams and hardware and software listings that differ from those submitted in the baseline configuration in reference (g).

3. HBSS version 3.6 is designated Mission Assurance Category (MAC) Level II and is authorized to process up to and including Sensitive information in the System High mode of operation while connected to the NIPRNET.

4. Per reference (e), all System Administrators (SA), including part-time or collateral duty SAs, will be certified and cleared to the level of information classification of a given information system. Contractor SAs will also meet certification and access control (to include personnel clearances and physical controls) requirements.

5. As per reference (b), the overall risk was identified as Low. In order to retain this ATC, the system owner is required to comply with all DoD and Marine Corps policy requirements for IA and ensure the items listed below are accomplished. Non-compliance may result in termination of this approval.

   a. Implementation and maintenance of personnel and technical security controls described in reference (g).

   b. Implementation and maintenance of the IA Vulnerability Management program required patches/fixes per reference (e).

   c. Compliance with requirements for proper protection of data and systems as defined by reference (f).

6. In accordance with the requirements of the Chairman Joint Staff Instruction (CJSI) 6211.02B Defense Information Systems Network (DISN) Policy, Responsibilities and Processes, 31 July 2003, we acknowledge that the Defense Information Systems Agency (DISA) will conduct periodic monitoring of our MCEN NIPRNET. We acknowledge and consent to DISA conducting an initial vulnerability assessment and periodic unannounced vulnerability assessments on our existing connected host systems to determine the security features in place to protect unauthorized access or attack and enhance IA posture.

7. Questions may be directed to the MCEN CAR at DSN 278-3418 or (703) 784-3418.

RAY A. LETTEER

Copy to:
MCNOSC

ENCLOSURE (13) EXAMPLE OF ACCREDITATION LETTER

Each Accreditation Decision Letter shall follow the respective templates and guidance supplied by the Navy or Marine Corps Designated Accrediting Authority (DAA). A sample letter is shown below:

UNITED STATES MARINE CORPS
MARINE CORPS SYSTEMS COMMAND
2200 LESTER ST
QUANTICO, VIRGINIA 22134-6050

IN REPLY REFER TO:

5000
Ser SGM 062/171
DEC - 4 2007

From: Director, Information Assurance and Joint Requirements
To: Marine Corps Network Operations Security Center (MCNOSC), 2032 Barnett Ave, Quantico, VA 22134

Subj: AUTHORITY TO OPERATE HOST BASED SECURITY SYSTEM (HBSS) VERSION 3.6.1.x

Ref: (a) DoDI 5200.40, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP)," 30 Dec 97
(b) DODD 8500.1 "Information Assurance," 24 Oct 02
(c) DoD Federal Information Security Management Act (FISMA), Electronic Government Act [Title III] of 17 Dec 02
(d) DODI 8500.2 "Information Assurance Implementation," 6 Feb 03
(e) CJCSI 6510.01D "Information Assurance (IA) and Computer Network Defense (CND)," 15 Jun 04
(f) MCEN OP Directive 007-04, "USMC Information Assurance/Vulnerability Management Program (IAVM)"
(g) Application Security Plan (ASP) for the HBSS, 12 Oct 07

1. Per references (a) through (f), and based on a review of reference (g), I hereby grant Authority to Operate (ATO) for the Host Based Security System (HBSS) with software version 3.6.1.x. This ATO is my formal declaration that a satisfactory level of security is present.

2. HBSS is authorized to process Sensitive But Unclassified (SBU) information in a System High security mode of operation for a period of *three (3)* years from the date of this letter. During this period, HBSS software version 3.6.1.x. will only be operated based on the mission/system description, data classification, security mode of operation, concept of operation, operating environment, and interconnections, as defined by reference (g) and at a level of risk for which the site Designated Approving Authority has assumed responsibility.

3. It is the responsibility of the MCNOSC to contact the Certification Authority (CA) within five days if the application

Subj: AUTHORITY TO OPERATE HOST BASED SECURITY SYSTEM (HBSS) VERSION 3.6.1.x

is in any way modified from that established in reference (g). This ATO is contingent on the following provisions:

a. HBSS is an application that resides at the MCNOSC. Its primary security measures are inherited from this platform and its continued operation is contingent upon the Data Center's accreditation.

b. Reference (c) requires annual validation of security controls and contingency plans. Submit required validation documents and date the validation was performed to this office annually.

c. References (e) and (f) require you to establish and maintain an Information Assurance Vulnerability Management Program to monitor and test Information Assurance Vulnerability Alerts (IAVAs) for impact to Marine Corps systems and/or applications. You are to manage IAVAs in accordance with the references noted in this paragraph.

4. Questions may be directed to the CA, Ms. Nancy Levesque, at (703) 432-3833, DSN 378-3833.

Michael F. Davis

M. F. DAVIS
Designated Approving Authority

2

ENCLOSURE (14) EXAMPLE OF IT SECURITY POA&M TEMPLATE

Plan of Action and Milestones (POA&M) Template

A POA&M is prepared for DoD ISs with a current ATO that are found to be operating with an open unresolved security deficiency through Government Accountability Office (IAGO) audits, Inspector General (IG) audits, or other reviews or events, such as an annual security review or compliance validation. POA&M is a tool identifying tasks that need to be accomplished to remediate any identified vulnerabilities in a program or system. The POA&M addresses: (1) why the system needs to operate; (2) any operational restrictions imposed to lessen the risk during the interim authorization; (3) specific corrective actions necessary to demonstrate that all assigned IACs have been implemented correctly and are effective; (4) the agreed upon timeline for completing and validating corrective actions; and (5) the resources necessary and available to properly complete the corrective actions. This section provides the instructions for filling out both the System level IT security POA&M and the Component level IT security POA&M.

There are three types of DoD IT Security POA&Ms, as reflected in the next table and further described in paragraphs below. Further instructions on completing the System Level POA&M and the DoD Component Level POA&M can be accessed by clicking on the links.

Types of DON IT Security POA&Ms

POA&M Type	Responsibility	Submit To	Dates
System Level POA&Ms	Program Managers (PM)/Information Assurance Managers (IAM)	Operational DAA, DON Deputy CIO (Navy), and DON Deputy CIO (Marines) for management. DON CIO: All systems with a CAT I weakness or on OMB Watch List (Exhibit 300s) for security and others on request.	1 December, 1 March, 1 June, 1 September
DON Component Level Significant IA Security Weaknesses POA&M	DON CIO	OSD(NII)	1 December, 1 March, 1 June, 1 September
DoD Enterprise POA&M	OSD(NII)	OMB	Included in the October FISMA Report

System Level IT Security POA&M

The System level IT Security POA&M is a living document designed to be a management tool to assist agencies in closing their security performance gaps, assist inspectors general (IGs) in their evaluation work of agency security performance, and assist OMB with oversight responsibilities. The System level IT Security includes all IT security weaknesses found during any other review done by, for, or on behalf of the agency including, but not limited to, Government Accountability Office (GAO) audits, financial system audits, official security test and evaluation or compliance review and critical infrastructure vulnerability assessments.

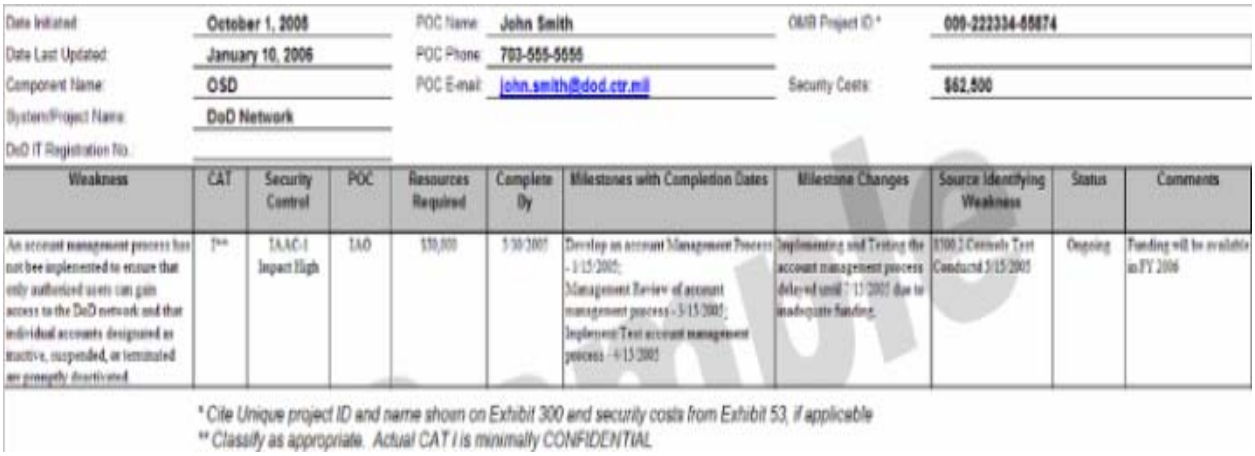
When there is compelling operational necessity, DoD information system may be allowed to operate despite IT security weakness that cannot be corrected or adequately mitigated within prescribed timeframes because of technology limitations or, in rare cases, prohibitive costs. Such instances must be fully justified, approved, and documented as described below.

The figure below is an example of a completed System level IT Security POA&M, illustrating the appropriate level of detail required. Included in the heading of the System level IT Security POA&M template is a field for OMB Project Identification (ID) and Security Costs which must be filled in from Exhibits 300 and 53, where applicable.

To download a Sample System Level IT Security POA&M Template, follow the URL below:

https://diacap.iaportal.navy.mil/ks/DIACAP%20Package/POAM/DIACAP%20Package.xls.zip

Sample System Level POA&M



Date Initiated:	October 1, 2008		POC Name:	John Smith		OMB Project ID *	000-222334-55674			
Date Last Updated:	January 10, 2006		POC Phone:	703-555-5555						
Component Name:	OSD		POC E-mail:	john.smith@dod.ctr.mil		Security Costs:	$62,500			
System/Project Name:	DoD Network									
DoD IT Registration No:										
Weakness	**CAT**	**Security Control**	**POC**	**Resources Required**	**Complete By**	**Milestones with Completion Dates**	**Milestone Changes**	**Source Identifying Weakness**	**Status**	**Comments**
An account management process has not bee implemented to ensure that only authorized users can gain access to the DoD network and that individual accounts designated as inactive, suspended, or terminated are promptly deactivated.	I**	IAAC-1 Impact High	IAO	$50,000	5/30/2005	Develop an account Management Process - 1/15/2005; Management Review of account management process - 3/15/2005; Implement/Test account management process - 4/15/2005	Implementing and Testing the account management process delayed until 7/1/2005 due to inadequate funding	8500.2 Controls Test Conducted 3/15/2005	Ongoing	Funding will be available in FY 2006

* Cite Unique project ID and name shown on Exhibit 300 and security costs from Exhibit 53, if applicable

** Classify as appropriate. Actual CAT I is minimally CONFIDENTIAL

The following instructions explain how a system level IT Security POA&M should be completed.

POA&M Instructions

Reference	**Instruction**
Column 1	Weakness. Type of security weakness. Describe security weaknesses identified during certification or by the annual program review, IG independent evaluation or any other work done by or on behalf of the program office or DoD Component. Sensitive descriptions of specific weaknesses are not necessary, but sufficient data must be provided to permit oversight and tracking. Where it is necessary to provide more sensitive data, the IT Security POA&M should note the fact of its special sensitivity and should be classified accordingly. Where more than one weakness has been identified, number each individual security weakness as shown in the examples. The DIACAP TAG has developed a set of statements of weakness that can be used for the weakness description.
Column 2	CAT (Severity Code). Code assigned to a system deficiency by a CA as part of certification analysis to indicate (1) the risk level associated with the deficiency and (2) the urgency with which the corrective action must be completed. Severity codes are expressed as "CAT I, CAT II, CAT III" where CAT I is the indicator of greatest risk and urgency. POA&Ms with CAT I weaknesses will normally be classified.
Column 3	Security Control. An IA Control describes an objective IA condition achieved through the application of specific safeguards or through the regulation of specific activities. The objective condition is testable, compliance is measurable, and the activities required to achieve the IA Control are assignable and thus accountable. IACs are assigned according to MAC and Confidentiality Levels in accordance with DoDI 8500.2.
Column 4	POC. Identity of the office or organization that the DoD Component will hold responsible for resolving the security weakness.
Column 5	Resources Required. Estimated funding or manpower (i.e., full time equivalents (FTE)) resources required to resolve the security weakness. Include the anticipated source of funding (i.e., within the system or as a part of a cross-cutting security infrastructure program). Include whether a reallocation of base resources or a request for new funding is anticipated. This

Reference	Instruction
	column should also identify other, non-funding, obstacles and challenges to resolving the security weakness (e.g., lack of personnel or expertise, development of new system to replace insecure legacy system, etc.).
Column 6	Scheduled Completion Date. Scheduled completion date for resolving the security weakness. Please note that the initial date entered should not be changed. If a security weakness is resolved before or after the originally scheduled completion date, the agency should note the actual completion date in Column 10, "Status." If risk is accepted for a CAT II or CAT III weakness, enter N/A.
Column 7	Milestones with Completion Dates. A milestone will identify specific requirements to correct an identified weakness. Mitigation plan (actions) will be listed as a milestone in column 7. Please note that the initial milestones and completion dates should not be altered. If there are changes to any of the milestones the agency should note them in the Column 8, "Milestone Changes."
Column 8	Milestone Changes. This column would include new completion dates for the particular milestone.
Column 9	Identified in GAO Audit or Other Review. The agency should identify the source (e.g., program review, IG audit, GAO audit, etc.) of the security weakness. Security weaknesses that have been identified as a significant IA security weakness or other reportable condition in the latest agency IG audit under other applicable law (e.g., financial system audit under the Financial Management Integrity Act, etc.) If yes is reported, also identify and cite the language from the pertinent audit report.
Column 10	Status. The DoD Component should use one of the following terms to report status of corrective actions: Ongoing, Completed or Risk Accepted for a CAT II or CAT III weakness that has been accepted by the DAA. "Completed" should be used only when a security weakness has been fully resolved and the corrective action has been tested. Include the date of completion or risk accepted for a CAT III weakness.
Column 11	Comments. Include any amplifying or explanatory remarks that will assist in understanding other entries relative to the weakness.

Once an initial system level IT Security POA&M weakness has been opened, no changes may be made to the data in columns 1 (Weakness), 6 (Scheduled Completion Data), 7 (Milestones with Completion Dates), and 9 (Identified in Chief Financial Officer (CFO) Audit or other Review).

Component Level IT Security POA&M

DoD Components are required to complete and submit a DoD Component level significant deficiency IT Security POA&M. A Component level IT Security POA&M is required for systemic weaknesses (significant deficiencies) identified across the Component, or systemic weaknesses (significant deficiencies) identified by GAO and IG audits and reviews.

The figure below contains an example of a completed Component level IT Security POA&M, illustrating the appropriate level of detail required. Once a DoD Component has completed the initial Component level IT Security POA&M, no changes should be made to the data in columns 1 (Weakness), 4 (Scheduled Completion Date), 5 (Milestones with Completion Dates), and 7 (Source Identifying Weakness).

The Component level IT Security POA&M should be filled out using the instructions above for a system level IT Security POA&M; however, the Security Control column does not apply for a Component level IT Security POA&M.

To download a Sample Component Level IT Security POA&M Template follow the URL listed below:

https://diacap.iaportal.navy.mil/ks/libraries/Reference%20Library/Templates/Component_Level_POAM_Template.xls.zip

Date Last Updated:	March 1, 2005	POC Name:	Mr. Navy CIO
Component Name:	OSD	POC Phone:	555-555-1234
		POC E-mail:	doncio@nav.mil

Weakness	POC	Resources Required	Scheduled Completion Date	Milestones with Completion Dates	Milestone Changes	Identified in CFO Audit or other Review	Status
Annual testng of contingency plans not being conducted	Component CIO	700K	5/30/2005	Verify and test contingency plans for 98% of systems C&A 12/30/05		Annual review	Ongoing
Security Awareness, Training, and Education - no process for tracking completion of specialized training	Component CIO	200K	11/30/2005	Implement and test training database 6/1/05; Enter personnel requiring specialized training into database 10/1/05		OIG Audit	Ongoing
Inconsistent and inadequate person computer Inventory afloat	Component CIO	500K	8/31/2005	Implement and test afloat computer inventory system 10/1/05; Enter 50% afloat inventory into database 3/1/06; Enter 100% afloat inventory into database 10/1/06		Naval Audit Service	Ongoing

ENCLOSURE (15) EXAMPLE OF STATEMENT OF COMPLIANCE

DEPARTMENT OF THE NAVY
<COMMAND/ORGANIZATION NAME>
<ADDRESS>

IN REPLY REFER TO:

ISSM/XX/XXXX
<DATE>

From: Commanding Officer, <ORGANIZATION NAME>
To: Commanding Officer, Naval Network Warfare Command
Network Security Director/DAA (Attn: Mr. Rich Voter)

Subj: INFORMATION ASSURANCE COMPLIANCE STATEMENT (ANNUAL REVIEW)

Ref: (a) DODD 8500.1
(b) DODI 8500.2
(c) DODI 8510.01
(d) IAVM Compliance
(e) DOD IA Policies
(f) DISN Connection Approval Policies
(g) DON IA Policies
(h) DON UTNPP
(i) DOD/DON PKI Policies
(j) DOD/DON Wireless Policies
(k) DOD/DON Malicious Software Policies

1. <ORGANIZATION NAME> recognizes the need for compliance with all Federal, Department of Defense (DOD), and Department of the Navy (DON) IA policies as promulgated in references (a) through (k).

2. <ORGANIZATION NAME> acknowledges that IA requirements have been or are being met in the ongoing deployment and/or life cycle management activities for the following servers:

<Server Name>
<Server Name>

3. If operational requirements prohibit compliance with the requirements identified in the policies and procedures outlined above, all appropriate exception and waiver process activities have been, or are being, implemented.

4. The <ORGANIZATION NAME> point of contact for this matter is <POC NAME> and can be reached at (XXX) XXX-XXXX, DSN XXX-XXXX.

Program Manager Date

Copy to:

NNWC
PMW 160IA