DEPARTMENT OF THE NAVY
CHIEF INFORMATION OFFICER
1000 NAVY PENTAGON
WASHINGTON DC 20350-1000

13 May 2009

MEMORANDUM FOR DEPARTMENT OF THE NAVY DEPUTY CHIEF INFORMATION OFFICER (NAVY)
DEPARTMENT OF THE NAVY DEPUTY CHIEF INFORMATION OFFICER (MARINE CORPS)
COMMANDER, NAVAL NETWORK WARFARE COMMAND

Subj: DEPARTMENT OF THE NAVY INFORMATION ASSURANCE AND CERTIFICATION AND ACCREDITATION PROCESS CONCEPT OF OPERATIONS

Ref: (a) DON CIO memo, Senior Information Assurance Officer Alignment and Responsibilities for Information Assurance and Certification and Accreditation Processes, of 18 Dec 08

Encl: (1) Department of the Navy Information Assurance and Certification and Accreditation Process Concept of Operations of 15 May 2009

As required by reference (a), enclosure (1) is promulgated.

The Department of the Navy Chief Information Officer points of contact for this action are Dr. Richard Etter, 703-602-6882, richard.etter@navy.mil; Ms. Sonya Smith, sonya.r.smith1@navy.mil, 703-604-7059; and Mr. Raymond Moon, raymond.l.moon@navy.mil, 703-601-1234.

Robert J. Carey

Copy to:
DON SIAO

Department of the Navy Information Assurance and Certification and Accreditation Process Concept of Operations 13 May 2009

Foreword

Information Technology (IT) is critical to the Department of the Navy's (DON) ability to achieve its mission. However, the ever-increasing threat to DON IT assets and information magnifies the importance of secure operations of systems and networks within the DON. The DON Chief Information Officer (CIO), in accordance with references (a), (b) and (c), is designated as the DON Senior Information Assurance Officer (SIAO), responsible for developing and managing the DON Information Assurance (IA) security program. Subsequently, per reference (d), the DON SIAO was tasked with implementing an integrated IA program. This Concept of Operations (CONOPS) expands upon, clarifies, and implements reference (e) to instantiate the business rules, and aligns the DON risk management and Certification and Accreditation (C&A) processes.

This CONOPS:

- Implements the policy for joint visibility and risk management, as it pertains to the C&A process to ensure appropriate alignment across the Department;

- Identifies roles and responsibilities of major process participants in the C&A process; and

- Describes the high-level interactions that must occur among the process participants for the DON's C&A process operates effectively and efficiently.

Table of Contents

Figures:

1. **Purpose**

a. This CONOPS describes the roles and responsibilities of the DON SIAO and the interaction between the Marine Corps Enterprise Network (MCEN) Designated Accrediting Authority (DAA), Navy Operational Designated Accrediting Authority (ODAA), and the DON SIAO. It also identifies the role of the DON Deputy CIOs (Navy and Marine Corps) in C&A management oversight.

b. All IT systems designated for use outside the DON and IT systems from other departments or agencies for use within the DON require coordination and participation of the DON SIAO and Service DAAs in the C&A process and risk management decision.

c. This CONOPS applies to the C&A process for General Service (GENSER) IT systems and does not address the C&A process supporting intelligence, Sensitive Compartmented Information (SCI), or Special Access Program (SAP) IT systems.

d. The Service DAAs shall: keep the DON SIAO and supporting staff informed of Service efforts related to the implementation of the IA program. The DON SIAO supports the Service DAAs in their risk management efforts.

2. **Background**

a. Establishing a consistent risk management methodology and C&A processes across the DON are key part of the DON IA program.

b. The DON SIAO, per reference (d), is tasked to establish and enforce the C&A process as part of the overall DON IA program. For clarity, certification includes the comprehensive evaluation of technical and non-technical security features of systems and networks based on IA policy and testing results. Certification identifies and assesses the residual risk of operating a system and the acceptable controls to correct or mitigate IA security weaknesses. Accreditation is the formal determination by the DAA of the risk of operating a system in a particular manner with appropriate safeguards in place to ensure the level of risk is acceptable.

c. To ensure this process is visible, transparent, consistent, and integrated, the DON must formalize and align the processes for both Services' C&A approval processes.

3. **Roles and Responsibilities**

a. DON SIAO. The responsibilities are specified in reference (e).

b. DON Deputy CIOs (Navy and Marine Corps). The DON Deputy CIOs (Navy and Marine Corps) are responsible for:

(1) Ensuring all enterprise-wide systems comply with requirements of applicable DON, Department of Defense (DoD), and Federal policies and mandates, such as references (a), (d), and (f) through (i);

(2) Tracking the C&A status of Navy and Marine Corps information systems that are governed by the DON IA program;

(3) Ensuring certification quality, capacity, visibility, and effectiveness;

(4) Facilitating a consistent application of IA policies, processes, responsibilities, and procedures across the Department;

(5) Determining with the DON SIAO that the DAA decision making processes are acceptable and consistently applied; and

(6) Overseeing and managing IA/C&A compliance evaluations and assessments.

c. Designated Accrediting Authority (DAA). Per references (d), (j) and (k), the DAA is the official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. This term is synonymous with Designated Approving Authority and Delegated Accrediting Authority. The DAA must understand the operational need for the system(s) and the operational consequences of not operating the system(s), as part of the risk management decision process. The DAA is responsible for:

(1) Granting interim and final authorization to operate (IATO/ATO) of a network or system in a specified security mode, and denying authorization to operate (DATO) when the network or system poses an unacceptable risk;

(2) Ensuring security is incorporated as an element of the information system life-cycle process;

(3) Ensuring the operational information system's security policies are in place for each system, project, program, and organization or site for which the DAA has authorization authority;

(4) Ensuring the establishment, administration, and coordination of security for systems that the DAA's command or organization operates; and

(5) Implementing IA requirements.

4. **DON C&A Information Flows – Inter-Service (Marine Corps and Navy) Accreditations**

a. Certification and accreditation packages for information systems designated for use in both the Navy and Marine Corps will be processed according to normal Navy and Marine Corps business rules. The Navy CA/ODAA or the MCEN CA/DAA will notify the DON SIAO of packages that meet the criteria for inter-Service accreditation. This allows for situational awareness and DON visibility into all inter-Service accreditations ready for an accreditation decision and gives the DON SIAO the opportunity to review documentation associated with the system. While the goal is to identify an IS early in the process as an inter-Service program, this may not always be known at the start of the C&A process. To accommodate this, at any point a participant of the C&A team (Program Manager (PM), Echelon II (EII)/Major Subordinate Command (MSC), CA, DAA, DON SIAO) discovers the information system is intended for use by both services, that party shall notify both Service DAAs and the DON SIAO. If the package is acceptable to both the Navy ODAA and the MCEN DAA, the accreditation decision is finalized by the responsible service and an accreditation approval endorsement is issued by the other service. The responsible service DAA will notify the DON SIAO of the accreditation. Normal business practices showing inter-service accreditation with concurrence are depicted in Figure 1.

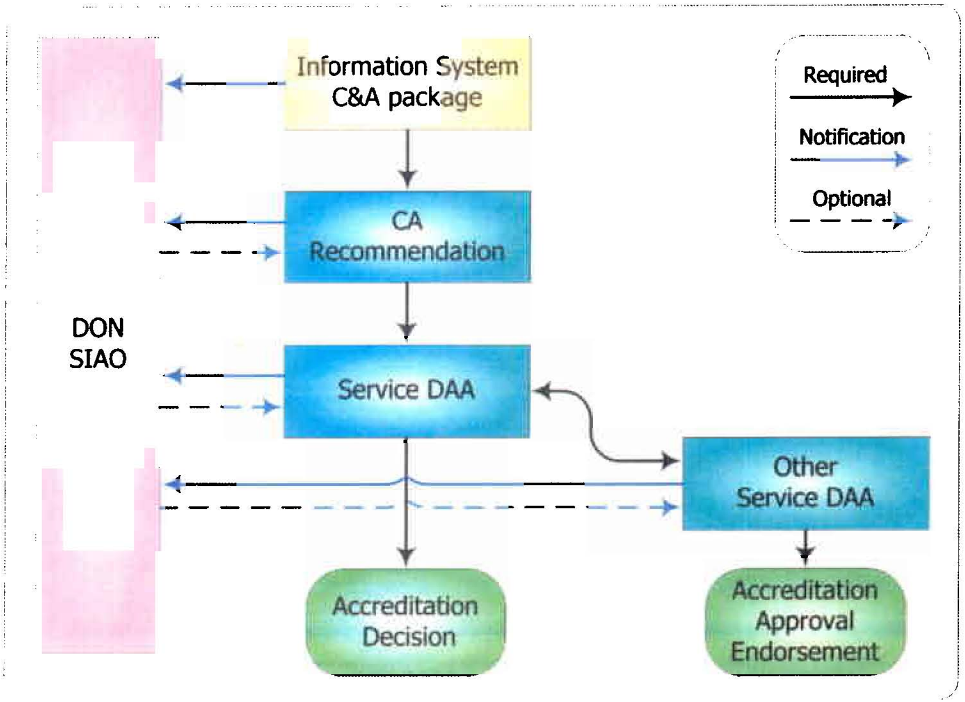

Figure 1. Inter-Service Accreditation with Concurrence

Figure 2 identifies the DON SIAO role in the C&A process when a DAA intends to deny authorization to operate for a system. This would occur when a DAA determines there is unacceptable level of unmitigated system risk. The Service DAAs will notify the DON SIAO of their intent to deny authorization to operate. The DON SIAO will work with the DAAs and others to resolve the differences to achieve the best results for the DON.

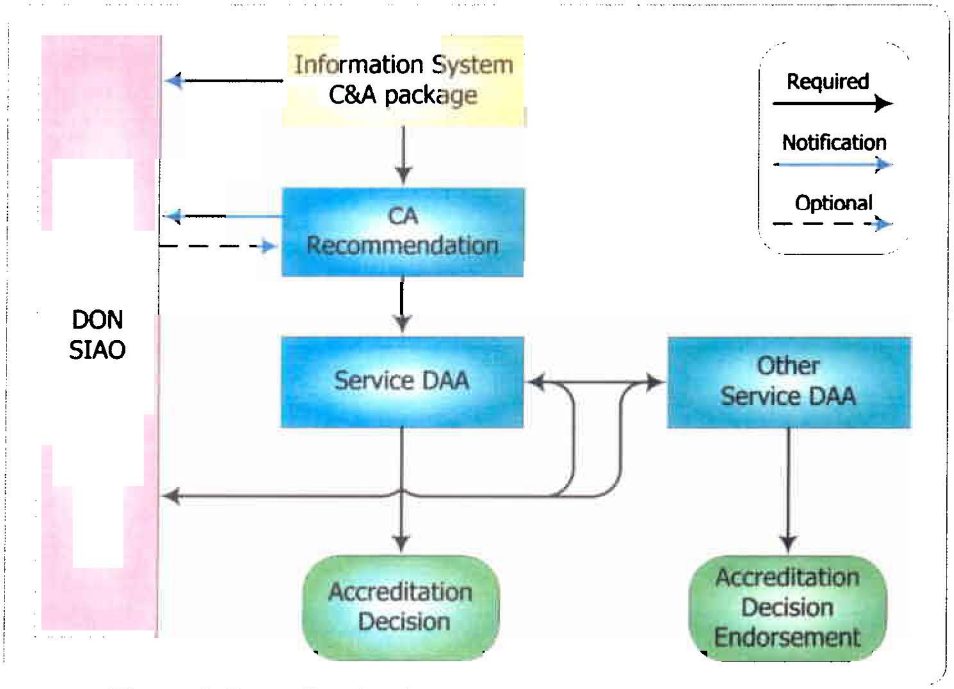

Figure 2. Inter-Service Accreditation without Concurrence

5. **DON C&A Information Flows – Inter-DoD (Marine Corps/Navy & External Combatant Commander, Service, and/or Agency) Accreditations**

a. For an IS owned and accredited by another Military Department, Agency, or a Combatant Command, requiring Navy or Marine Corps acceptance of an accreditation decision, the DAA (Navy ODAA or MCEN DAA) is responsible for evaluating that accreditation decision. The respective DAA will use the certification artifacts associated with the IS to make the accreditation decision.

b. The Navy and Marine Corps CAs and DAAs will notify the DON SIAO of packages that meet the criteria for inter-DoD accreditation, allowing for situational awareness and Department visibility into all inter-DoD accreditations. The DON SIAO will have the opportunity to review documentation associated with the system. The notifications will occur upon initial entry, CA recommendation, and reciprocity concurrence. The Service DAAs, once they have a recommended accreditation decision, shall notify the DON SIAO of their intent. The Service DAAs will not issue their decision until the DON SIAO acknowledges this intent. The time that DON SIAO has to acknowledge is 72 hours from receipt of notification of intent. If the DON SIAO does not acknowledge within 72 hours, DAAs will issue their accreditation decision. Figure 3 shows the process for systems accredited within the DON and utilized by other DoD components.

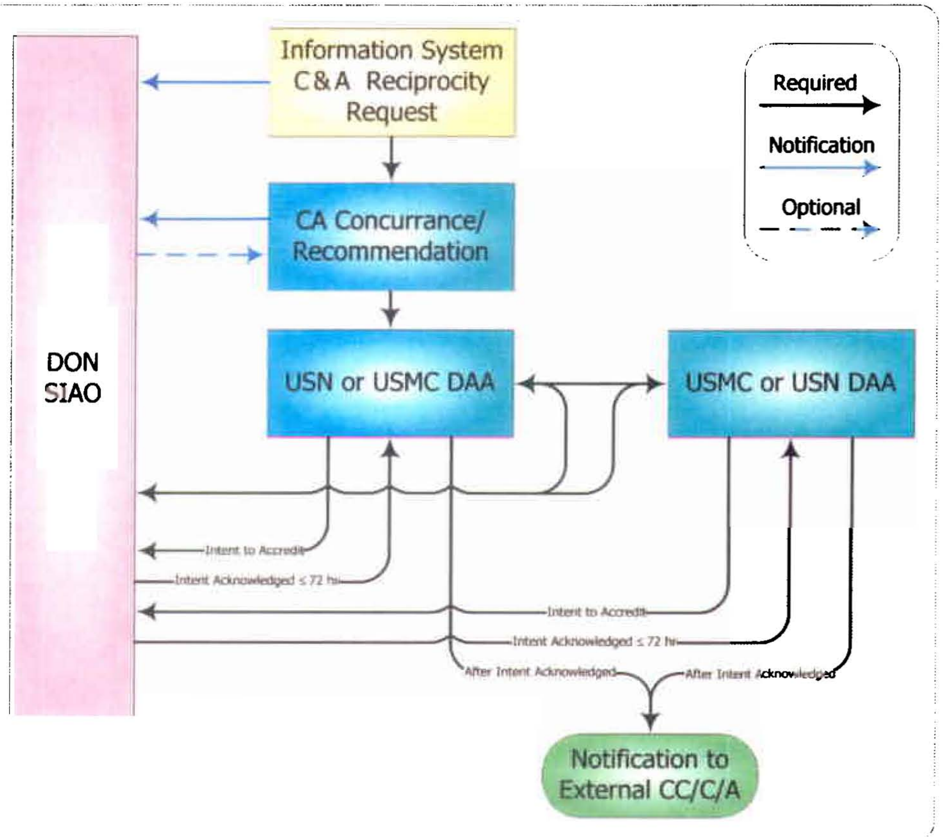
Information System C&A Reciprocity Request
Required
Notification
Optional
CA Concurrance/ Recommendation
DON SIAO
USN or USMC DAA
USMC or USN DAA
Intent to Accredit
Intent Acknowledged ≤ 72 hrs
Intent to Accredit
Intent Acknowledged ≤ 72 hrs
After Intent Acknowledged
After Intent Acknowledged
Notification to External CC/C/A

Figure 3. Inter-DoD (Marine Corps/Navy & External Combatant Commander, Service, and/or Agency) Accreditations

c. For inter-Service accreditations described above, the DAA(s) will notify the DON SIAO should an IS present unacceptable risk to the Navy or Marine Corps before issuing a denial of authorization to operate. For these situations, the respective DON Deputy CIO (Navy/Marine Corps) and the DON SIAO will work with the Military Departments, Agency, or Combatant Command to resolve the unacceptable risk. If an agreement cannot be reached with the external organization, the DON SIAO, and the respective DAA will present the issue to the Principal Accrediting Authorities (PAAs) for resolution.

d. While the goal is to identify an IS as an inter-DoD program early in the process, this may not always be known at the start of the C&A process. To accommodate this, at any point a participant of the C&A team (Program Manager (PM), Echelon II (EII)/Major Subordinate Command (MSC), CA, DAA, DON SIAO) discovers the information system is coming in to or going out of the DON, that party shall notify both Service DAAs and the DON SIAO.

6. **DON Information Assurance Council (IAC)**

a. In December 2007, the DON SIAO established the Information Assurance Council (IAC), chaired by the DON Deputy SIAO, to coordinate and collaborate on IA matters and issues. The IAC meets monthly and membership includes the MCEN DAA, Navy ODAA and DON Deputy CIO Navy (OPNAV N61) representative.

b. The DON SIAO will use the IAC as the venue for addressing and resolving risk management and C&A issues. In the event an issue requires senior level attention, the DON Deputy SIAO will coordinate with IAC members to set up a meeting with the DON SIAO and the Service Flag level DAAs to resolve the issue. Members of the IAC are responsible for briefing their respective senior leadership on the issues prior to the meeting. IAC members can raise an issue at any time and are not limited to the monthly meetings. Additionally, the IAC will maintain the DON IA and C&A process concept of operations to ensure it evolves with continuous process improvements.

References

a. Federal Information Security Management Act of 2002, Title 11 of E-Government Act of 2002, PL 107-347, (codified in sections of 40, 44 U.S.C.)

b. OMB memo, M-09-02, Information Technology Management Structure and Governance Framework, of 21 Oct 08

c. DON CIO memo, Designation of the Department of the Navy Senior Information Assurance Officer, of 11 Jan 05

d. DoDINST 8510.01, DoD Information Assurance Certification and Accreditation Process (DIACAP)

e. DON CIO memo, Senior Information Assurance Officer Alignment and Responsibilities for Information Assurance and Certification and Accreditation Processes, of 18 Dec 08

f. SECNAVINST 5430.7P, Assignment of Responsibilities and Authorities in the Office of the Secretary of the Navy

g. Clinger-Cohen Act of 1996 (Title 40), USC Title 10 et seq)

h. DoDINST 8500.01E, Information Assurance

i. DoDINST 8500.2, Information Assurance Implementation

j. CJCSM 6510.01, Defense-In-Depth: Information Assurance (IA) and Computer Network Defense (CND), of 25 Mar 03

k. SECNAVINST 5239.3A, Department of the Navy Information Assurance (IA) Policy, of 20 Dec 2004