



**DEPARTMENT OF THE NAVY**

CHIEF INFORMATION OFFICER  
1000 NAVY PENTAGON  
WASHINGTON DC 20350-1000

18 December 2008

**MEMORANDUM FOR DON DEPUTY CHIEF INFORMATION OFFICER (NAVY)  
DON DEPUTY CHIEF INFORMATION OFFICER (MARINE  
CORPS)**

**Subj: SENIOR INFORMATION ASSURANCE OFFICER ALIGNMENT AND  
RESPONSIBILITIES FOR INFORMATION ASSURANCE AND CERTIFICATION  
AND ACCREDITATION PROCESSES**

- Ref:**
- (a) Federal Information Security Management Act of 2002, Title III 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) SECNAVINST 5430.7P, Assignment of Responsibilities and Authorities in the Office of the Secretary of the Navy
  - (f) Clinger-Cohen Act of 1996 (Title 40), USC Title 10 et seq)
  - (g) DoDINST 8500.01E, Information Assurance
  - (h) DoDINST 8500.2, Information Assurance Implementation

1. Information Technology (IT) is critical to the Global War on Terrorism and the Department of the Navy's (DON) ability to achieve its mission. However, the ever-increasing threat to the DON's IT assets and information magnifies the importance of ensuring secure operations of systems and networks within the DON. The DON Chief Information Officer (CIO), in accordance with references (a) and (b), is designated as the DON's senior agency information security officer to develop and manage the Department's Information Assurance (IA) security program. Reference (c) tasked the DON SIAO with ensuring an integrated DON IA program.

2. A key part of the DON IA program is establishing a consistent risk management methodology and certification and accreditation (C&A) processes across the DON. The DON Senior Information Assurance Officer (SIAO), per reference (d), is tasked to establish and enforce the C&A process as part of the overall Component 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 declaration, by the appropriate DAA authorizing the system, to operate in a particular manner with appropriate safeguards in place to ensure the level of risk, as determined by the certifying authority, is acceptable. To ensure this process is visible, transparent, consistent, and integrated, the Department must formalize and align the processes for both certification and accrediting approval processes. Accordingly, per references (d) and (e), the DON SIAO is responsible for:

Subj: SENIOR INFORMATION ASSURANCE OFFICER ALIGNMENT AND RESPONSIBILITIES FOR INFORMATION ASSURANCE AND CERTIFICATION AND ACCREDITATION PROCESSES

- a. Ensuring all enterprise-wide systems comply with requirements of applicable DON, Department of Defense (DoD), and Federal policies and mandates such as references (a) and (d) through (g);
- b. Serving as the single IA coordination point with the DON Service DAAs for implementation and accreditation of Joint or Defense-wide applications on DON enterprise networks or to DoD Component enclaves.
- c. Establishing a reporting relationship and ensuring alignment between the Navy and Marine Corps DAAs;
- d. Tracking the C&A status of information systems that are governed by the DON IA program via an automated C&A tool;
- e. Formally delegating Certifying Authority (CA) duties;
- f. Ensuring certification quality, capacity, visibility, and effectiveness;
- g. Facilitating a consistent application of IA policies, processes, responsibilities, and procedures across the Department;
- h. Ensuring communication between the DON SIAO, Service level DAAs, and network operations of the Services;
- i. Establishing and enforcing the C&A process for applications residing on DON enterprise networks, e.g., NGEN; and
- j. Ensuring the consistent application of waiver request standards and processing across DON enterprise networks.

3. In achieving and ensuring the activities in paragraph 2 are carried out, specifically, the consistent C&A enforcement and risk management processes within the DON, the following tiered business rules are to be followed:

- a. For Service-specific systems/applications that shall be used in either the Navy or the Marine Corps but not both, the respective Service DAA shall issue the accreditation decision, and provide an informational copy, including the supporting risk analysis, within working three days, to the DON SIAO.
- b. For DON enterprise systems/applications/networks that shall be used in both the Navy and the Marine Corps, the Service DAAs shall conduct the reviews necessary to make the accreditation decision for their respective Service, then forward their recommendations to accredit to the DON SIAO. The service DAAs shall collaborate with the DON SIAO to develop a consensus based decision on DON-wide systems/applications. Absent any consensus, the DON

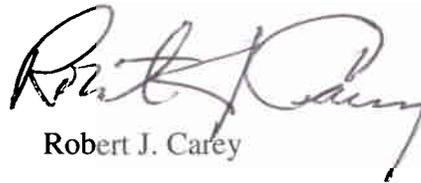
Subj: SENIOR INFORMATION ASSURANCE OFFICER ALIGNMENT AND RESPONSIBILITIES FOR INFORMATION ASSURANCE AND CERTIFICATION AND ACCREDITATION PROCESSES

SIAO may issue an accreditation decision if the Service DAA accreditation recommendations are not in agreement.

c. For DoD and external systems/applications that Services need to install on DON enterprise networks, the DON SIAO shall collaborate with both Service DAAs to conduct the reviews necessary to make an accreditation decision on behalf of the DON user base. Absent any consensus, the DON SIAO may issue an accreditation decision if the Service DAA accreditation recommendations are not in agreement.

4. In accordance with the business rules in paragraph 3, the Navy Operational DAA, Marine Corps Enterprise DAA, and the DON SIAO shall coordinate development and codification of the certification and accreditation approval processes within 120 days of this memorandum, to ensure the appropriate alignment across the Department. This shall include the detailed processes on how to issue accreditation decisions based on the scope of the system or application's interfaces to other systems and applications, decision criteria, risk metrics, as well as on the breadth of the system or application's user base, for example, Navy-only users, Marine Corps-only users, DON-wide users, or authorized DoD users.

5. Questions concerning this guidance may be directed to Dr. Richard Etter, DON Deputy SIAO for Computer Network Defense (CND), at (703) 602-6882, [richard.etter@navy.mil](mailto:richard.etter@navy.mil).



Robert J. Carey