



DEPARTMENT OF THE NAVY

CHIEF INFORMATION OFFICER
1000 NAVY PENTAGON
WASHINGTON DC 20350-1000

27 September 2007

MEMORANDUM FOR DISTRIBUTION

**Subj: ROLES AND RESPONSIBILITIES OF THE DEPARTMENT OF THE NAVY
DEPUTY SENIOR INFORMATION ASSURANCE OFFICER FOR COMPUTER
NETWORK DEFENSE (DON DEPUTY SIAO FOR CND)**

- Ref:**
- (a) Subtitle III of Title 40, United States Code [Recodification of the Clinger-Cohen Act at 40 U.S.C. 11101 et seq.]
 - (b) Title 10 United States Code, Section 2223, Information Technology: Additional Responsibilities for Chief Information Officers
 - (c) Federal Information Security Management Act (FISMA) of 2002, Title III of E-Government Act of 2002 (PL 107-347)
 - (d) SECNAVINST 5430.7N, Assignment of Responsibilities and Authorities in the Office of the Secretary of the Navy, of 9 Jun 05
 - (e) SECNAVINST 5239.3A, Department of the Navy Information Assurance (IA) Policy, of 20 Dec 04
 - (f) DON CIO memo, Designation of the Department of the Navy Senior Information Assurance Officer, of 11 Jan 05

Encl: (1) Duties and Responsibilities of the Department of the Navy Deputy Senior Information Assurance Officer (SIAO) for Computer Network Defense (DON Deputy SIAO for CND)

One of the permanent goals of the Department of the Navy (DON) is to improve and enhance the security of our networks. Information technology (IT) is an integral force multiplier and enables the successful execution of a myriad of missions in the DON. As such, the security of IT networks and applications is paramount to successful execution of the DON mission.

The DON Chief Information Officer (CIO) is required by references (a) through (e) to ensure that information assurance (IA) and network security status in the DON is maintained, managed, and subsequently reported to the Secretary of the Navy and the Under Secretary of the Navy. Further, the DON CIO is required to ensure that external organizations (such as the Department of Defense Chief Information Officer (DoD CIO), the Office of Management and Budget (OMB), and the Government Accountability Office (GAO)) and other DoD and DON audit agencies are kept informed and their efforts are coordinated.

In reference (f), the DON CIO designated the DON Deputy CIO (Policy and Integration) as the DON Senior Information Assurance Officer (SIAO). The DON SIAO was established to facilitate alignment and consistent application of Information Management (IM), IT, and IA policies, processes, responsibilities, and procedures across the Department. The DON SIAO provides oversight and ensures maintenance of network security throughout DON networks.

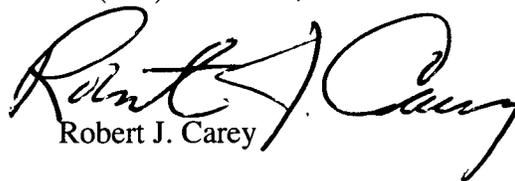
Subj: ROLES AND RESPONSIBILITIES OF THE DEPARTMENT OF THE NAVY
DEPUTY SENIOR INFORMATION ASSURANCE OFFICER FOR COMPUTER
NETWORK DEFENSE (DON DEPUTY SIAO FOR CND)

As the Department conducts more missions in a net-centric environment, there is a growing need to ensure alignment and consistent application of security practices across the DON. References (a) through (e) provide guidance to the DON regarding IA and network security. Adhering to the required levels of IA and network security with agility requires further alignment of processes across the Department. The DON security practices also require further integration with DoD and other Components (Combatant Commands, Department of the Army, Department of the Air Force, and DoD Agencies).

To improve and align the DON computer network defense (CND) efforts, I am establishing the position of the DON Deputy SIAO for CND. I hereby appoint the DON CIO Information Assurance and Network Security Team Lead as the DON Deputy SIAO for CND. The DON Deputy SIAO for CND will coordinate with the Assistant for Administration Office of the Under Secretary of the Navy (AAUSN), Navy and Marine Corps developmental and operational DAAs, and the DON Deputy CIOs (Navy and Marine Corps) to improve and align the DON CND efforts and ensure that a consistent IA and security process is delivered across the Department. The roles and responsibilities for the position of the DON Deputy SIAO for CND are included in enclosure (1).

The DON Deputy SIAO for CND will report to the DON SIAO and be responsible for maintaining unified and enhanced DON CND processes, establishing policy, and providing appropriate oversight of the processes.

My point of contact is Richard Etter (703) 602-6882, richard.etter@navy.mil.



Robert J. Carey

Distribution:

Immediate Office of the Secretary (ASN (M&RA), ASN (RD&A), ASN (I&E), ASN (FM&C),
AAUSN)

Dept of the Navy Staff Offices (OPA, JAG, OLA, CHINFO, AUDGEN, CNR, NAVINSGEN)

OGC

CNO

CMC

DON Deputy CIO (Navy)

DON Deputy CIO (Marine Corps)

COMNAVNETWARCOM

**Duties and Responsibilities of the
Department of the Navy Deputy Senior Information Assurance Officer for Computer Network
Defense (DON Deputy SIAO for CND)**

The DON Deputy SIAO for Computer Network Defense (CND) duties and responsibilities include, but are not to be limited to:

1. Align and coordinate network risk management across the DON.
2. Develop a consistent certification and accreditation (C&A) process across the DON to facilitate reduced cycle time, improved reliability and improved security across DON networks.
3. Establish a DON enterprise IA posture in a risk-shared environment that allows for risk 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.
4. Ensure that DON CIO and DON SIAO are kept abreast of significant items (e.g., major mission degradation, shared lessons learned, and IA strategies) across the Enterprise.
5. Encourage a robust program within the DON for vulnerability assessments and penetration testing, including effective use of red team exercises.
6. Encourage sharing of CND lessons learned and best practices across the Navy and Marine Corps.
7. Ensure timely analysis of CND trends to shape DON policy.
8. Collaborate with all the DAAs for AAUSN, the Navy, and Marine Corps; and representatives of the DON Deputy CIO (Navy and Marine Corps), to coordinate DAA issues, ensure consistent guidance is provided, and discuss and resolve problem areas.
9. Coordinate efforts to achieve and maintain the DON in the GREEN status of the President's Management Agenda (at least 90 percent compliance) with the Federal Information Security Management Act (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.
10. Ensure proper reporting under FISMA. IT networks, applications, and systems must complete a C&A in accordance with the DoD 8500 series and all IT systems must be registered in DITPR-DON.
11. Coordinate and align assignment of the mission assurance category (MAC) for information systems, preferably during the acquisition and development process.

12. Coordinate and align processes for determining and approving the classification level required for the applications implemented on information systems.
13. Identify and align commands responsible for responding to Cyber attacks or incidents.
14. Direct and align protective measures within the DON computer networks through network management and IA organization, procedures, tools and trained workforce.