



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

DON CIO Memo 01-09
January 30, 2009

MEMORANDUM FOR DISTRIBUTION

Subj: DEPARTMENT OF THE NAVY CHIEF INFORMATION OFFICER MEMORANDUM
01-09, INFORMATION ASSURANCE POLICY FOR PLATFORM INFORMATION
TECHNOLOGY

Ref: (a) DoD Directive 8500.01E, Information Assurance (IA), of 24 Oct 02
(b) DoD Instruction 8500.2, Information Assurance (IA) Implementation, of 6 Feb 03
(c) DoDI 8580.1, Information Assurance (IA) in the Defense Acquisition System,
of 9 Jul 04
(d) DoD Instruction 8510.01, DoD Information Assurance Certification and Accreditation
Process (DIACAP), of 28 Nov 07

Encl: (1) Platform Information Technology (PIT) Definitions for the Department of the Navy
(2) Department of the Navy Platform IT Information Assurance Guidance

1. Purpose. To establish the Department of the Navy (DON) Information Assurance (IA) Platform IT (PIT) policy and establish guidance for implementing the DON PIT policy at enclosure (2).

2. Background. Reference (a), paragraph E2.1.16.4, defines Platform Information Technology as computer resources, both hardware and software, that are physically part of, dedicated to, or essential in real time to the mission performance of special-purpose systems. Paragraph 2.3 of reference (a) states that reference (a) does not apply to PIT, where there is no platform IT interconnection. Reference (a) acknowledged that PIT presented IA risk management challenges different from automated information systems (AIS) and enclaves. Reference (a) is focused on Global Information Grid (GIG) protection and addresses IA requirements for PIT interconnection to the GIG. Reference (b) lists IA controls and describes procedures for applying integrated, layered protections of information systems and networks that fall under reference (a). Reference (c) requires that IA be integrated into the acquisition of systems and services within the Department of Defense (DoD). Reference (d) establishes the DoD Information Assurance Certification and Accreditation Process (DIACAP) as the DoD IT system certification and accreditation (C&A) process for systems that interconnect to the GIG.

The DON Chief Information Officer (CIO) began, in February 2007, a multi-phased approach to develop policy and processes for ensuring PIT systems have appropriate IA capabilities embedded within the system and the IA objectives are documented and validated. This document represents the completion of the PIT initiative by providing comprehensive policy and guidance for ensuring IA is incorporated into PIT for the DON. This document supersedes the PIT guidance contained in the Navy Certification Authority Certification Guide dated May 2007 and the Navy Certification Authority "Clarification of PIT for Navy Information Systems" dated 6 February 2007.

Subj: DEPARTMENT OF THE NAVY CHIEF INFORMATION OFFICER MEMORANDUM
01-09, INFORMATION ASSURANCE POLICY FOR PLATFORM INFORMATION
TECHNOLOGY

3. Discussion. This memorandum will be incorporated into a future DON directive addressing IA requirements for PIT.

Enclosure (1) provides definitions of key PIT related terms. Enclosure (2) provides IA guidance on the PIT designation process and the implementation of a PIT risk management program within the Department. This policy, with its enclosures, meets the DON goal to ensure implementation of IA into PIT, thereby meeting the intent of references (a) and (c).

All DON Information Systems (IS) must meet IA requirements of references (a) and (c), as appropriate, (i.e., the tenets of IA must be incorporated through a vigorous risk management process in all DON IT). The DON PIT IA Guidance of enclosure (2) provides a standardized process to ensure consistent application and review of IA requirements in PIT.

4. Policy

a. PIT Designation

(1) In order for an IS to be considered PIT, the Program Manager (PM) must follow the DON PIT IA Guidance in enclosure (2), which identifies the PIT designation procedures, and for PIT designated systems, the mandated risk management procedures. Only IS designated by the appropriate Designated Accrediting Authority (DAA) as PIT, in accordance with the process specified in enclosure (2), will be recognized as PIT.

(2) Any IS, including legacy systems, designated as PIT by someone other than the recognized DAAs stated below, will be required to obtain a DAA PIT designation within 24 months of policy issuance to continue to be recognized as PIT.

(a) IS operating strictly in the research, development, test, and evaluation (RDT&E) environment (with no connection to the SIPRnet/NIPRnet) may be designated as PIT by the Research & Development (R&D) DAA.

(b) IS operating in the Service operational environment are required to be designated PIT by the Navy Operational DAA (ODAA) or Marine Corps Enterprise DAA (MCEN DAA).

(c) For systems that shall be used in both the Navy and Marine Corps, the Navy ODAA and MCEN DAA shall conduct the reviews necessary to make the PIT determination for their respective Service, then forward their PIT recommendations to the DON Senior Information

Subj: DEPARTMENT OF THE NAVY CHIEF INFORMATION OFFICER MEMORANDUM
01-09, INFORMATION ASSURANCE POLICY FOR PLATFORM INFORMATION
TECHNOLOGY

Assurance Officer (SIAO). The Service DAAs shall collaborate with the DON SIAO to develop a consensus based decision on DON enterprise PIT systems.

(3) IS designated as PIT, that are planned for deployment outside the DON environment, must address PIT designation and IA requirements in a Memorandum of Agreement between the DON and the external organization to ensure recognition of the DON PIT designation and associated IA process requirements.

(4) Reference (a) identifies that stand-alone systems are required to comply with DIACAP unless they are categorized as PIT. If a stand-alone system meets the requirements to be designated as PIT, the DON PIT policy shall be followed.

b. PIT IA Requirements. DoD policy requires that IA shall be implemented in all IS and Service acquisitions. Reference (c) requires the PM to ensure IA is fully integrated into all phases of acquisition, upgrade, or modification programs, including initial design, development, testing, fielding, and operation. All PIT IS should start with the minimum set of IA controls delineated in reference (b), based on system Mission Assurance Category (MAC) and Confidentiality Level (CL) and follow the IA processes in enclosure (2).

c. PIT IA Approval

(1) Compliance with the DON PIT IA Guidance at enclosure (2) ensures that DON leadership understands the security state of the system and explicitly accepts the resulting risk to operations and assets prior to operation and/or deployment.

(2) All PIT IS must have their IA controls documented and validated prior to operation and/or deployment. Legacy and deployed PIT IS, which at the time of the policy issuance have a Navy ODAA/MCEN DAA PIT designation letter, are required to obtain a PIT authorization to operate (ATO) within 24 months of policy issuance, in accordance with the requirements identified in this policy and processes in enclosure (2).

(3) The Navy ODAA/MCEN DAA may delegate, in writing, authorization to grant PIT ATOs to a "PIT DAA." The DAA designation letter must specify PIT DAA requirements prior to the PIT DAA having authorization to grant PIT ATOs. The PIT DAA may also be designated, in the same letter, the Developmental and/or Research and Development DAA for a Command.

(4) A PIT ATO, when granted in accordance with this policy, will be accepted and recognized by all organizations within the DON.

Subj: DEPARTMENT OF THE NAVY CHIEF INFORMATION OFFICER MEMORANDUM
01-09, INFORMATION ASSURANCE POLICY FOR PLATFORM INFORMATION
TECHNOLOGY

(5) After IS transition to the operating forces, the operational commanders assume responsibility for maintaining the system's configuration and operations in accordance with the systems' approved documentation. Program sponsors with life cycle accountability for the fielded systems are responsible for providing support for transitioned systems.

d. PIT Reporting Requirements

(1) IS are required to be reported in the DoD Information Technology Portfolio Registry - DON (DITPR-DON) in accordance with the current DON DITPR-DON Guidance (located on the DON CIO web site), regardless of the applicability of C&A requirements. Once an IS is officially designated as PIT, and if it meets the DITPR-DON registration requirements, then DITPR-DON must be updated to show the "C&A Required" data element response as "No" and the "C&A Required Not Apply Explanation" data element response as "Without Platform IT Interconnection."

(2) Once an IS has received formal designation as PIT in accordance with the process of enclosure (2), the PM must maintain a copy of the PIT designation letter. The designation letter must also be uploaded into DITPR-DON.

Questions concerning this policy may be directed to Dr. Richard Etter, DON CIO Information Assurance and Critical Infrastructure Protection Team Leader, 703-602-6882, richard.etter@navy.mil.



Robert J. Carey

Distribution:
ASN (RD&A)
DON Deputy CIOs (Navy and Marine Corps)
COMUSFLTFORCOM
COMUSNAVEUR
COMPACFLT
USNA
COMUSNAVCENT
COMNAVRESFORCOM
COMNAVVAIRSYSCOM
BUMED
NETC

DON CIO Memo 01-09
January 30, 2009

Subj: DEPARTMENT OF THE NAVY CHIEF INFORMATION OFFICER MEMORANDUM
01-09, INFORMATION ASSURANCE POLICY FOR PLATFORM INFORMATION
TECHNOLOGY

Distribution: (continued)

COMNAVSEASYSKOM

FLDSUPPACT

COMNAVSUPSYSKOM

DIRSSP

CNIC

COMNAVLEGSVCCOM

NAVPGSCOL

COMNAVFACEKGCOM

COMNAVSAFECEN

BUPERS

NAVWARCOL

COMUSNAVSO

ONI

COMNAVSPECWARCOM

COMSPAWARSYSKOM

COMNAVDIST

NAVHISTCEN

NAVY BAND

COMOPTVFOR

COMNAVNETWARCOM (Attn: ODAA, N5)

COMMARFOREUR

COMMARCORSYSKOM

COMMARFORPAC

COMMARFORLANT

COMMARFORRES

MCNOSC

MCCDC