



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

DON CIO Memo 02-10
26 April 2010

MEMORANDUM FOR DISTRIBUTION

Subj: DEPARTMENT OF THE NAVY CHIEF INFORMATION OFFICER MEMORANDUM 02-10, INFORMATION ASSURANCE POLICY UPDATE FOR PLATFORM INFORMATION TECHNOLOGY

Ref: (a) Department of the Navy Chief Information Officer Memorandum 01-09, Information Assurance Policy for Platform Information Technology, of 30 Jan 2009
(b) DoD Directive 8500.01E, Information Assurance (IA), of 24 Oct 02
(c) DoD Instruction 8500.2, Information Assurance (IA) Implementation, of 6 Feb 03
(d) DoD Instruction 8580.1, Information Assurance (IA) in the Defense Acquisition System, of 9 Jul 04
(e) 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 update the Department of the Navy (DON) Information Assurance (IA) policy for Platform IT (PIT), reference (a). The DON PIT definitions and guidance for implementing the DON PIT policy at enclosures (1) and (2) are unchanged from what was issued by reference (a).

Nothing in this policy shall alter or supersede the existing authorities and policies of the Director of Naval Intelligence regarding the protection of sensitive compartmented information and special access programs for intelligence.

2. Background. Reference (b), 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 (b) states that reference (b) does not apply to PIT where there is no platform IT interconnection. Reference (b) acknowledged that PIT presented IA risk management challenges that are different from automated information systems (AIS) and enclaves. Reference (b) is focused on Global Information Grid (GIG) protection and addresses IA requirements for PIT interconnection to the GIG. Reference (c) lists IA controls and describes procedures for applying integrated, layered protections of information systems and networks that fall under reference (b). Reference (d) requires that IA be integrated into the acquisition of systems and services within the Department of Defense (DoD). Reference (e) 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.

Subj: DEPARTMENT OF THE NAVY CHIEF INFORMATION OFFICER MEMORANDUM
02-10, INFORMATION ASSURANCE POLICY UPDATE FOR PLATFORM
INFORMATION TECHNOLOGY

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 supersedes the DON IA policy for Platform IT dated 30 January 2009, 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.

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.

All DON Information Systems (IS) must meet IA requirements of references (b) and (d), 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, are required to obtain a DAA PIT designation by 30 January 2011 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 RDT&E DAA, but that designation is only valid within the RDT&E environment. If the PIT system is required to leave the RDT&E environment, a PIT designation decision from the Navy Operational DAA (ODAA) or Marine Corps Enterprise Network DAA (MCEN DAA) must be obtained.

Subj: DEPARTMENT OF THE NAVY CHIEF INFORMATION OFFICER MEMORANDUM
02-10, INFORMATION ASSURANCE POLICY UPDATE FOR PLATFORM
INFORMATION TECHNOLOGY

(b) IS operating in or connecting to the Service operational environment are required to be designated PIT by the Navy ODAA or 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 Assurance Officer (SIAO). The Service DAAs shall collaborate with the DON SIAO to develop a consensus based decision on DON enterprise PIT systems.

(3) The PM is required to notify the DAA that granted the PIT designation (Navy ODAA, MCEN DAA, or RDT&E DAA) of changes which will result in a modification to the system architecture to determine if the change impacts the validity of the PIT designation prior to implementation. System architecture change includes additional components, changes to external connections (both PIT-to-PIT Interconnections and Platform IT Interconnections), or any hardware or software changes that modify, or add new system functionality.

(4) 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.

(5) Reference (b) requires stand-alone systems 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 IA implementation in all IS and Service acquisitions. Reference (d) requires the PM to ensure IA is fully integrated into all phases of acquisition, upgrade, or modification programs, including initial design, development, testing, fielding, operation, sustainment, and disposal. All PIT IS will start with the minimum set of IA controls delineated in reference (c), based on system Mission Assurance Category (MAC) and Confidentiality Level (CL) and follow the IA processes in enclosure (2).

c. PIT IA Risk 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, deployment, and sustainment.

(2) All PIT IS must have their IA controls and all interconnections (both internal and external) documented and validated prior to operation and/or deployment.

Subj: DEPARTMENT OF THE NAVY CHIEF INFORMATION OFFICER MEMORANDUM
02-10, INFORMATION ASSURANCE POLICY UPDATE FOR PLATFORM
INFORMATION TECHNOLOGY

(3) Legacy and deployed PIT IS, which had a Navy ODAA/MCEN DAA PIT designation letter when reference (a) was issued in January 2009, are required to obtain a PIT Risk Approval (PRA) (formerly referred to as a PIT Authorization to Operate (ATO) in reference (a)) by 30 January 2011, in accordance with the requirements identified in this policy and processes in enclosure (2). In the context of PIT, the term PRA functionally replaces the certification and accreditation term ATO used in reference (a) and enclosure (2) to describe the document accepting the PIT IA risk prior to operation. PIT IS that received a PIT designation after January 2009 have 24 months from receipt of the PIT designation to obtain a PRA.

(4) The Navy ODAA/MCEN DAA may delegate, in writing, authorization to grant PRAs to a "PIT DAA." The DAA designation letter must be issued prior to the PIT DAA having authorization to grant PRAs.

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

(6) PRA requirements:

(a) PRAs will remain valid as long as the IA posture does not change. An IA posture change includes, but is not limited to, system architecture changes, or any other change that increases risk or degrades the security posture. Any IA posture change must be provided to the DAA that approved the PRA for impact review on that risk approval. When an IA posture changes, the PIT IS may be required to go through the risk approval process again to obtain a new PRA for the new configuration.

(b) A periodic review of the PRA by the approving DAA is required. At the time the PRA is granted, the approving DAA will establish the periodic review schedule not to exceed four years. The periodic review schedule may coincide with the Fleet Response Plan deployment schedule for the afloat platform provided that it does not exceed four years between reviews for a given PIT IS configuration.

(c) At the time PRA is granted, the Navy ODAA/MCEN DAA must be notified if a delegated PIT DAA has granted the approval.

(7) Interim PRA:

(a) In limited circumstances, PIT IS may be granted an interim PRA. The Interim PRA is limited to a maximum of one year and is only permitted to fulfill documented operational need or to ensure fixes can be fielded to previously deployed PIT IS. At the time an interim approval is granted, the Navy ODAA/MCEN DAA must be notified if a delegated PIT DAA has granted the approval.

Subj: DEPARTMENT OF THE NAVY CHIEF INFORMATION OFFICER MEMORANDUM
02-10, INFORMATION ASSURANCE POLICY UPDATE FOR PLATFORM
INFORMATION TECHNOLOGY

(b) PIT IS with interim PRAs must develop a Plan of Actions & Milestones (POA&M) on how they will reach full risk approval within the interim period. PIT IS with interim PRAs must be reviewed at least every 90 days to ensure adequate progress is being made on the POA&M.

(c) If a PIT IS cannot obtain a final approval within the interim timeline, the system must be removed from operation until final approval can be obtained or until an interim extension is approved by DON CIO. Only DON CIO may approve interim PRAs that exceed one year. DON CIO will only consider approving PRAs for greater than a year when Flag-level endorsement of the request and demonstrated operational need are provided. It is unlikely that the DON CIO will approve interim operation of a PIT system beyond the period of one year.

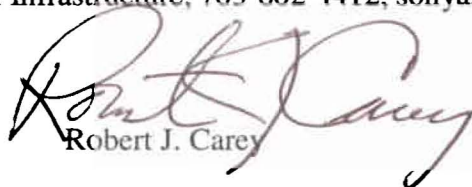
(8) After IS transition to the operating forces, the operational commander assumes responsibility for maintaining the system's configuration and operates it in accordance with the systems' approved documentation. Program sponsors with life cycle accountability for the fielded systems are responsible for providing support for transitioned systems including, but not limited to, IA vulnerability management and critical software patch support.

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 for the life of the system. The designation letter must also be uploaded into DITPR-DON.

5. Questions. Questions concerning this policy may be directed to Ms. Sonya Smith, DON CIO Director, Cybersecurity and Critical Infrastructure, 703-602-4412, sonya.r.smith1@navy.mil.



Robert J. Carey

Distribution:
ASN (RD&A)
DON Deputy CIOs (Navy and Marine Corps)

Subj: DEPARTMENT OF THE NAVY CHIEF INFORMATION OFFICER MEMORANDUM
02-10, INFORMATION ASSURANCE POLICY UPDATE FOR PLATFORM
INFORMATION TECHNOLOGY

Distribution: (continued)

COMFLTCYBERCOM
COMUSFLTFORCOM
COMUSNAVEUR
COMPACFLT
USNA
COMUSNAVCENT
COMNAVRESFORCOM
COMNAVAIRSYSCOM
BUMED
NETC
COMNAVSEASYS
COMNAVSEASYS
FLDSUPPACT
COMNAVSUPSYSCOM
DIRSSP
CNIC
COMNAVLEGSVCCOM
NAVPGSCOL
COMNAVFACENCOM
COMNAVSAFECEN
BUPERS
NAVWARCOL
COMUSNAVSO
ONI
COMNAVSPECWARCOM
COMSPAWARSYSCOM
COMNAVDIST
NAVHISTCEN
NAVY BAND
COMOPTVFOR
COMNAVVCYBERFOR
COMNAVNETWARCOM (Attn: ODAA, N5)
COMMARFOREUR
COMMARCORSSYS
COMMARFORPAC
COMMARFORLANT
COMMARFORRES
MCNOSC
MCCDC