



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

24 September 2003

MEMORANDUM FOR DISTRIBUTION

Subj: INFORMATION TECHNOLOGY (IT) POLICY GUIDANCE FOR FISCAL YEAR 2004
EXPENDITURES

As the Department of the Navy team achieves its vision of network centric operations and knowledge dominance, it is imperative that investment and expenditure decisions by Navy and Marine Corps commands are aligned with the goals of Naval Power 21, Sea Power 21, FORCENet and the DON IM/IT Strategic Plan. There are a number of DoD/DON policies, cited below, that promote alignment of Departmental IT efforts to ensure that secure, interoperable and standards-based solutions are implemented in a cost effective and timely manner. A footnote referencing this memorandum will be included in the FY2004 Program Authorization Documents.

Application, Data and Portfolio Management

- Applications and databases that are to be developed or procured must be registered in the DON Application and Database Management System (DADMS) and approved by the appropriate Functional Area Manager (FAM). There is a FAM appointed for each functional area, or "line of business" in the Department, with the authority to direct migration, consolidation, or retirement of applications and databases; develop and manage IT applications and database portfolios; and ensure that technology strategies are aligned with business and administration processes and warfighting strategies. The DADMS registration and FAM approval processes are meant to ensure that the DON achieves and maintains the consolidation and standardization necessary for network-centric operations. For more detail on the FAM initiative, see Under Secretary of the Navy memorandum "Designation of Department of the Navy Functional Area Managers" of 14 May 2002. The complete list of FAMs can be found in SECNAVINST 5000.36. Both documents are viewable at <http://www.doncio.navy.mil>.
- Applications that are listed in DADMS as FAM Disapproved or Allowed with Restrictions must focus their expenditures on retirement or migration (see CNO WASHINGTON DC 211902Z JUL 03). Further information concerning DADMS is available on the DADMS home page, <http://www.dadms.navy.mil>.
- The VCNO has directed (in CNO WASHINGTON DC 211902Z JUL 03) that Navy NMCI seats may only be ordered with software applications listed in DADMS as FAM Approved or Allowed with Restrictions.
- To foster interoperability across the DON and preclude the Department's being tied to a single vendor's solution, the DON Policy on the Use of Extensible Markup Language (XML) of 13 December 2002 (posted for reference at <http://www.doncio.navy.com>) prohibits use of proprietary extensions to XML-based specifications in DON IT systems.

Subj: INFORMATION TECHNOLOGY (IT) POLICY GUIDANCE FOR FISCAL YEAR 2004 EXPENDITURES

- Commercial software procurements must comply with Defense Federal Acquisition Regulation Supplement (DFARS) Subpart 208.74 and DODD 5000.2, paragraph E4.2.7. Additionally, commercial software procurements must comply with the SmartBUY Federal government-wide enterprise software-licensing project by following one of the procedures outlined in the USD (AT&L) and ASD (NII) policy memorandum "Department of Defense (DoD) Support for the SmartBUY Initiative" dated 16 Sep 2003. Pertinent references are posted on the ESI website (<http://www.don-imit.navy.mil/esi>).

Smart Card Technology

- The Deputy Secretary of Defense, in the memorandum "Smart Card Adoption and Implementation" of 10 Nov 1999, designated the common access card (CAC) as DoD's primary physical access badge and carrier of public key infrastructure (PKI) digital credentials. To ensure compliance with the intent of the memo and maintain interoperability with other Defense components, DON activities procuring physical access systems, card badging systems and other smart card technology must consider using the CAC as their primary means to gain physical access to DoD facilities (except for highly sensitive areas like SCIFs) and logical access to unclassified websites and networks. Additionally, DON activities considering procurement of smart card technology other than the CAC (i.e., for financial electronic purse or contactless physical access transactions) must obtain DON eBusiness Operations Office (Mechanicsburg, PA) approval of their initiatives and conform to DON smart card configuration management requirements. These DoD and DON policy requirements are outlined in DODD 8190.3 and the DON Smart Card and PKI policy memorandum of 19 May 2003 (posted as DON SC-PKI Policy on the Policy and Guidance page at <http://www.doncio.navy.mil>).
- Per ASN (RD&A) memorandum "Smart Card Reader Requirement" of 3 Jun 2003 and DON CIO memorandum "Information Technology-Related Procurements With Smart Card Readers" of 30 Apr 2002 (see <http://www.doncio.navy.mil>), all desktop/laptop computers procured by the DON for connection to the unclassified network services/NIPRNET must include smart card readers compatible with the DoD common access card (CAC).

Information Assurance (IA) and Public Key Enablement (PKE)

- National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 11, "National Information Assurance Acquisition Policy" (http://www.niap.nist.gov/cc-scheme/nstissp_11.pdf) and DoD Instruction 8500.2, "Information Assurance (IA) Implementation" (http://www.dtic.mil/whs/directives/corres/pdf/i85002_020603/i85002p.pdf) established National and DoD policy for the procurement of IA and IA enabled commercial off the shelf (COTS) and government off the shelf (GOTS) products. An IA enabled product is one that provides security services as a *feature* rather than as the primary functionality of

Subj: INFORMATION TECHNOLOGY (IT) POLICY GUIDANCE FOR FISCAL YEAR 2004 EXPENDITURES

the product. A list of available products is available at <http://www.niap.nist.gov/cc-scheme>. DON CIO memorandum dated 1 July 2003 requires all procurements of IA and IA enabled products to comply with National and DoD policy.

- Assistant Secretary of Defense (ASD) memorandum “Public Key Enabling (PKE) of Applications, Web Servers, and Networks for the Department of Defense (DoD)” of 17 May 2001 (<http://www.dod.mil/nii/org/sio/ia/pki/documents.html>) establishes DoD policy for Public Key Enabling of DoD applications. All DoD unclassified applications, web servers and networks that authenticate users must be PK enabled, unless exempted by the DoD policy memo cited above.

The following information is provided as notice of policy that will be implemented in the near future that may affect your IT planning:

- DON Navy Marine Corps Portal (NMCP) Policy Number 1 requires that constituent portals incorporate NMCP integration and architecture into their system design. NMCP Policy Number 2 will take steps to control portal proliferation and redundant investment in portal development. The intent is to have a single Navy Marine Corps Portal environment, and investment in existing portals should be carefully considered pending additional guidance on the NMCP architecture, standards and content management.
- Section 208 of the E-Government Act and OMB Circular A-11 require Federal Agencies to conduct Privacy Impact Assessments (PIAs) before developing or procuring IT systems that collect, maintain, or disseminate information in an identifiable form from or about the public. Information in an identifiable form refers to data that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means. OMB will shortly be issuing final implementing guidance. For the text of the E-Government Act, see http://www.cio.gov/documents/e_gov_act_2002.pdf. OMB Circular A-11 may be found at <http://www.whitehouse.gov/omb/circulars/a11/02toc.html>.

Questions concerning the above requirements or the Department’s enterprise implementation planning may be directed to Mike LeValley, DON CIO Investment Management and Implementation Planning Team Lead, at (703) 602-6847.



D. M. Wennergren

Distribution:
CNO (N09B, N6, N61)
CMC (DMCS, C4)
CHNAVPERS
COMLANTFLT
COMPACFLT

Subj: INFORMATION TECHNOLOGY (IT) POLICY GUIDANCE FOR FISCAL YEAR 2004
EXPENDITURES

Distribution: (Continued)

COMNAVEUR
COMUSNAVCENT
COMSC
COMNAVRESFOR
COMNAVMETOCOM
COMNAVSECGRU
COMNAVNETWARCOM
BUMED
COMNAVVAIRSYSCOM
COMSPAWARSYSCOM
COMNAVFACENGCOM
COMNAVSUPSYSCOM
COMNAVSEASYSYSCOM
ONI
NETC
NAVSTKAIRWARCEN
DIRSSP
COMNAVSPECWARCOM
NCTSI
COMOPTEVFOR
COMNAVSYSMGTACT

Copy to:

Immediate Office of the Secretary (ASN(M&RA), ASN(RD&A), ASN(I&E), ASN(FM&C) (FMO)
(FMB-B))

OGC

CNO (N82)