



DEPARTMENT OF THE NAVY

CHIEF INFORMATION OFFICER
1000 NAVY PENTAGON
WASHINGTON, DC 20350-1000

19 September 2006

MEMORANDUM FOR DISTRIBUTION

Subj: DEPARTMENT OF THE NAVY (DON) INFORMATION TECHNOLOGY (IT)
POLICY GUIDANCE FOR FISCAL YEAR (FY) 2007 EXPENDITURES

In FY 2007, as in recent years, our information management/information technology (IM/IT) efforts will focus on creation of a joint, net-centric environment that delivers knowledge dominance to Naval warfighters. To that end, we must invest only in projects that are aligned with the Department's strategic vision and aimed at our goal of a secure, interoperable architecture, providing web-enabled services and full dimensional protection. Department of the Navy (DON) commands and activities must comply with this guidance, where applicable, in order to release and/or obligate FY 2007 funds for IM/IT investments.

1. Business Transformation (aka 'BMMP') Certification Requirement

Effective 1 October 2005, 10 U.S.C. 2222 (as added by Section 332 of the Ronald W. Reagan National Defense Authorization Act (NDAA) for Fiscal Year 2005) prohibits obligation of funds for any defense business system modernization that will have a total cost in excess of \$1 million unless it has been reviewed and certified by the appropriate Office of the Secretary of Defense (OSD) Investment Review Board (IRB) and approved by the Defense Business System Modernization Committee (DBSMC). The DON Business Information Technology System Pre-Certification Workflow Guidance, Version 2.0 (downloadable from <http://www.doncio.navy.mil>) establishes the DON process to obtain pre-certification per DoD implementing guidance for all Tier 1, 2 and 3 Defense Business System Modernizations. 10 U.S.C. 2222 (a link to the text is provided at [http://www.doncio.navy.mil/\(yvlefm45yulbqtejp52wrdbu\)/contentview.aspx?ID=1639&ShowMore=true](http://www.doncio.navy.mil/(yvlefm45yulbqtejp52wrdbu)/contentview.aspx?ID=1639&ShowMore=true).) specifically provides that obligation of funds for a defense business system modernization that has a total cost in excess of \$1 million in the absence of a prior approved certification is a violation of the Anti-deficiency Act, 31U.S.C.1341(a)(1). Therefore, no FY 2007 funds for the acquisition, development, or modernization of an IT business system may be obligated without a prior approved certification if the total cost of the development/ modernization effort will exceed \$1 million. POC for BMMP certification questions is [REDACTED] (703) 607-5671, or [REDACTED]

2. IT Budget (NITE/STAR) Registration

Section 332 of the Ronald W. Reagan National Defense Authorization Act (NDAA) for FY 2005 also requires that each Defense Business System (DBS) be reported separately in the IT budget exhibits and that the IT budget exhibits reflect the amounts budgeted for development/modernization and current services for those DBSs. Accordingly, no FY 2007 funding (includes Navy Working Capital Fund (NWCF) costs and capital budget authority) may be obligated for a DBS unless that DBS has been assigned an 'AIS/Ext'

Subj: DEPARTMENT OF THE NAVY (DON) INFORMATION TECHNOLOGY (IT)
POLICY GUIDANCE FOR FISCAL YEAR (FY) 2007 EXPENDITURES

for current/future reporting in the DON IT budget database (NITE/STARweb). POC is
[REDACTED] (703) 692-4841, [REDACTED]

3. DADMS/DITPR-DON Registration

- NAVADMIN 124/05 (viewable at <http://www.npc.navy.mil/ReferenceLibrary/Messages>) established the requirement for networks, servers, and associated network devices to be registered in the Department of the Navy Application and Database Management System (DADMS). Additionally, it required that FAM “Approved”, “Approved - Interim Waiver”, and “AWR” applications be linked only to registered servers and to report the termination of server applications not FAM “Approved”, “Approved – Interim Waiver” or “AWR” in DADMS. In FY 2007, as in 2006, a Business Case Analysis (BCA), DADMS registration, and designation as “Approved” by the Enterprise Services FAM must be completed before there is a network, server or associated device procurement or block upgrade to existing networks, servers, or associated devices. In FY 2007, no development, modernization, operation, or maintenance of unregistered networks, servers, or associated devices is authorized. Accordingly, no FY 2007 funds (includes NWCF costs and capital budget authority) may be obligated for the acquisition, development, modernization, operation, or maintenance of unregistered networks, servers, or associated devices.
- No development, modernization, operation, or maintenance of software applications that are not registered in the DON variant (DITPR-DON) of Defense Information Technology Program Registry and not designated “Approved” or “Approved – Interim Waiver” (Navy) or “Allowed With Restrictions” (Marine Corps) by the appropriate Functional Area Manager (FAM) is authorized, nor may an application be connected to a DON network without DITPR-DON registration and FAM permission. Accordingly, no FY 2007 funds (includes NWCF costs and capital budget authority) may be obligated for any application not registered in DITPR-DON and not designated “Approved” or “Approved – Interim Waiver” or “Allowed With Restrictions”.
- The DoD IT Portfolio Registry (DITPR) and DoD SIPRNet Registry Annual Guidance for 2006 (DITPR Guidance) requires that all Mission Critical (MC), Mission Essential (ME), and Mission Support (MS) IT systems and all Defense Business Systems (DBS) be registered in DITPR, the DoD SIPRNet IT Registry, or the Intelligence Community (IC) IT Registry, as appropriate, not later than 30 September 2006. Definitions of the criteria that qualify projects as IT systems for this purpose are included in Appendix C of the DITPR Guidance. The DON vehicle for registering DON systems in DITPR is DITPR-DON, which uploads to DITPR. In order to ensure compliance with OSD policy, no FY 2007 funds (including NWCF costs and capital budget authority) may be obligated for any MC, ME or MS IT

Subj: DEPARTMENT OF THE NAVY (DON) INFORMATION TECHNOLOGY (IT)
POLICY GUIDANCE FOR FISCAL YEAR (FY) 2007 EXPENDITURES

system or DBS that is not registered in DITPR-DON. POC for DITPR-DON registry questions is [REDACTED] (703) 602-6845, or [REDACTED]

- Tier 4 and Non-Tier systems must complete all data elements that DITPR-DON is configured to accept not later than 15 November 2006. Accordingly, no more than 12.5 percent of total budgeted FY2007 development/modernization (DEV/MOD) and current services funding (including NWCF costs and capital budget authority) may be obligated for Tier 4 and Non-Tier systems until all available data elements are completed in DITPR-DON.

4. Certification and Accreditation (C&A) of DON IT Assets

DoDD 8500.1 (Information Assurance) specifies that DON IT assets with connectivity to the Global Information Grid (GIG) or other DoD/DON networks require C&A in accordance with DoDI 5200.40 (DoD Information Technology Security Certification and Accreditation Process (DITSCAP) or its successor, the Defense Information Assurance Certification and Accreditation Process (DIACAP)), to be issued in late 2006). With the ever-increasing threat to DON IT assets, obtaining full accreditation in an Authority to Operate (ATO) must be a top priority for every IT asset owner. DON CIO message 031456Z MAY 06, provides DON policy concerning DITSCAP C&A requirements. If security deficiencies exist but operational demands make it necessary to award an Interim ATO (IATO), a waiver request accompanied by a Plan of Action and Milestones (POA&M) detailing a plan for elimination of each outstanding security deficiency to achieve full ATO status must be submitted to the DON Senior Information Assurance Officer (DON Deputy CIO for Policy Integration), via the appropriate Service's Designated Approval Authority and DON Deputy CIO (Navy or Marine Corps). POA&M process guidance is contained in the DON FISMA Guidance of March 2006, available on the DON CIO website (<http://www.doncio.navy.mil>). In that regard, for systems with FY 2007 DEV/MOD funding, no FY 2007 DEV/MOD funds may be obligated until an ATO or approved waiver is obtained. For systems with no DEV/MOD funding, FY 2007 obligations for 'current services' (i.e., maintenance) are limited to 25 percent of the budgeted FY 2007 current services figure until an ATO or approved waiver is obtained. DON CIO Naval message 151611Z SEP 06 provides amplifying guidance on systems not covered by this requirement. POC: [REDACTED] (703) 602-6202, or [REDACTED]

5. Application, Data and Portfolio Management

- XML - To ensure interoperability across the DON and preclude tying the Department 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.mil>, prohibits use of proprietary extensions to XML-based specifications in DON IT systems.

Subj: DEPARTMENT OF THE NAVY (DON) INFORMATION TECHNOLOGY (IT)
POLICY GUIDANCE FOR FISCAL YEAR (FY) 2007 EXPENDITURES

- DON XML NDR - All Navy and Marine Corps commands developing systems using XML should apply the development guidance and standards identified in the DON XML Naming and Design Rules (DON XML NDR). Adherence is necessary to maximize interoperability and enable a net-centric environment across the Department. The DON XML NDR may be viewed at <http://www.doncio.navy.mil>.

6. ESI/SmartBUY

Commercial software agreements have been established that coordinate multiple IT investments to leverage the Federal Government's purchasing power for best-priced, standards-compliant products. These agreements are managed through the DoD Enterprise Software Initiative (ESI) and the Federal SmartBUY program. SmartBUY does not mandate use of particular brands of software, but DON activities purchasing software for which agreements have been awarded must use the SmartBUY agreements. Agreements are currently in place for ESRI, Manugistics, Novell, WinZip, ProSight, and Oracle database products. (Oracle database products and options must be purchased via SmartBUY. Other Oracle products may also be ordered via SmartBUY.) These, and all future SmartBUY agreements will be publicized through the DoD ESI website, <http://www.esi.mil>. DON activities shall comply with Defense Federal Acquisition Regulation Supplement (DFARS 208.74), DODI 5000.2, "Operation of the Defense Acquisition System," paragraph E4.2.7 (links to both references at <http://akss.dau.mil/jsp/default.jsp>), and the USD AT&L - DoD CIO Joint Policy memorandum dated 22 December 2005, "Department of Defense (DoD) Support for SmartBUY Initiative" (http://www.esi.mil/uploaded_documents/0924GUE45834.doc), when acquiring commercial software.

7. USN Oracle License

A Navy-wide Oracle database enterprise license has been established through ESI/SmartBUY, providing all Navy employees ashore and afloat, including authorized support contractors, the right to use the Oracle database product. The enterprise license enables transition from older or unsupported versions of Oracle database products, and its use is mandatory where Oracle has been selected as the database solution. POC for ESI and enterprise licensing is [REDACTED] (703) 607-5658, [REDACTED]

8. USMC Enterprise Agreements

The Marine Corps has established enterprise license agreements for the software products listed below. Details on procurements of these products can be found in the corresponding MARADMIN. POC for these enterprise agreements is [REDACTED] (703) 432-5155 or [REDACTED]

Subj: DEPARTMENT OF THE NAVY (DON) INFORMATION TECHNOLOGY (IT)
POLICY GUIDANCE FOR FISCAL YEAR (FY) 2007 EXPENDITURES

- a. Oracle – MARADMIN 225/04
- b. Microsoft – MARADMIN 363/05
- c. Cognos – MARADMIN 530/05
- d. Redhat – MARADMIN 064/06

9. Navy Server Policy

The ASN(RD&A) memorandum of 12 November 2004, “Purchase of Servers and Application Hosting Services” stipulates that no new or upgraded servers or application hosting services are to be purchased, leased, or rented at any level of the Navy organization for CONUS (Continental United States) ashore use without the prior written approval of PEO-IT (or its successor, PEO EIS). The restriction extends to purchase, lease, or rental of servers or application hosting services under support contracts. Servers and application hosting for Top Secret information, compartmentalized information, and cryptologic activities related to National Security Systems are specifically excluded. The policy memorandum may be viewed at <https://peoeisportal.nmci.navy.mil/main>.

10. Internet Protocol Version Six (IPv6)

All assets being developed, procured, or acquired for the Global Information Grid (GIG) must be Internet Protocol Version Six (IPv6) capable and must be interoperable with IPv6 systems/capabilities. This explicitly includes all acquisitions that reached Milestone C after 1 October 2003. The current version of the DoD Information Technology Standards Repository (DISR) is viewable at <https://disronline.disa.mil/a/DISR/index.jsp>. DoD policy on IPv6 is stated in DoD CIO memoranda of 9 June 2003 and 29 September 2003, viewable at <http://iase.disa.mil/policy.html>.

11. Mobile Voice and Data Services

The Department is engaged in initiatives to reduce the costs of handheld wireless communications services. The ASN(RD&A) memorandum of 7 March 2005, “Department of the Navy Acquisition Policy on Mobile (Cellular) Phone and Data Equipment and Services,” requires that all wireless communication support for Navy or Marine Corps activities in CONUS (Alaska and Hawaii excepted) must be obtained via the nationwide contracts awarded by Fleet Industrial Supply Activity San Diego (FISCSD) or the Navy Marine Corps Intranet (NMCI). The memorandum allowed for continuation of contracts extant at the time the policy was signed until expiration, or 1 October 2005, whichever came first. The policy does not apply to secure communications devices. Waiver authority resides with PEO EIS. Further information about the policy, answers to frequently asked questions, links to ordering services, waiver request procedures, and a .pdf file of the policy memo may be found at <https://peoeisportal.nmci.navy.mil/main>.

Subj: DEPARTMENT OF THE NAVY (DON) INFORMATION TECHNOLOGY (IT)
POLICY GUIDANCE FOR FISCAL YEAR (FY) 2007 EXPENDITURES

12. Electronic Invoices for Telecommunications Services

The DON policy on electronic submission of payment requests provides guidance governing receipt of invoices from telecommunications service providers. All telecommunications service providers shall be required to submit their invoices in electronic format. Electronic billing affords the Department significant benefits, including more accurate and timely payment of bills, ease of auditing, and the ability to maintain an accurate inventory of services provided. Telecommunications services covered under this policy include all landline and wireless (cellular) voice and data circuits, and services acquired either directly through service providers or via an intermediary agent (e.g., DITCO, GSA) acting on behalf of the Department. Information regarding electronic data interchange (EDI) formats is available on the Internet at <http://www.X12.org>. EDI implementation guides are available on the Internet at <http://www.dod.mil/dfas/contractorpay/electroniccommerce/electronicdatainterchangeedi.html>.

13. Voice Over Internet Protocol (VOIP)

VoIP is an option for converged voice and data transmission. To ensure consistent architecture, standards and security across the DON enterprise, activities are directed to coordinate with the DON Deputy CIO Navy or Marine Corps, as appropriate, before employing a VoIP solution other than the NMCI solution.

14. Smart Card Technology

Access Control Systems/CAC – The Common Access Card (CAC) is designated the official physical and logical access badge for the Department of Defense (DoD), and carries DoD Public Key Infrastructure (PKI) credentials. Homeland Security Presidential Directive-12 (HSPD-12), signed by the President on 27 August 2004, established the requirement for a common standard for identification credentials issued to Federal employees and eligible contractors. DoD will ensure the CAC meets HSPD-12 mandates and associated Personal Identity Verification (PIV) standards. DON activities procuring access control systems and other smart card technology must use the CAC as the primary means to gain physical and logical access and ensure access control systems meet the technical requirements outlined in Federal Information Processing Standards (FIPS) 201-1. DON CIO must pre-approve procurement of smart card technology other than the CAC. DON Smart Card-PKI policy is available on the DON CIO website at <https://www.doncio.navy.mil/>. The PIV standard (FIPS 201-1) and supporting documents relative to HSPD-12 are available at <http://csrc.nist.gov/npivp>. POC: [REDACTED]
[REDACTED] (703) 601-0081, [REDACTED]

Subj: DEPARTMENT OF THE NAVY (DON) INFORMATION TECHNOLOGY (IT)
POLICY GUIDANCE FOR FISCAL YEAR (FY) 2007 EXPENDITURES

15. Information Assurance (IA) and Public Key Infrastructure/Public Key Enablement (PKI/PKE), Wireless Technology Security

- IA-enabled Product Acquisition – DoD Instruction 8500.2 (DoD Information Assurance Implementation), viewable at <http://www.dtic.mil/whs/directives/corres/html/85002.htm>, requires that all IA and IA-enabled products acquired meet the Common Criteria National Information Assurance Partnership (NIAP) framework, per NSTISSP Policy 11 (National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products). NSA and NIST-sponsored laboratories perform certification testing, which increases product acquisition costs. If there is no Common Criteria protection profile for an IT-enabled product (such as a Personal Digital Assistant), the Department will perform a similar product vetting with DITSCAP (or its successor, DIACAP) before allowing its connection to DON networks. POC: [REDACTED] (703) 602-6882, [REDACTED]
- Biometric Collection Systems – All new acquisitions or upgrades of electronic biometric collection systems used by DON activities to collect biometric data must conform with the DoD Electronic Biometric Transmission Specification (EBTS) (v1.1), of 23 August 2005, and be interoperable with the DoD Automated Biometric Identification System (per DoD Directive 4630.5 (Interoperability and Supportability of IT and National Security Systems). The EBTS can be found at http://www.biometrics.dod.mil/Documents/DoD_ABIS_EBTS.pdf. POC: [REDACTED] (703) 601-0081, [REDACTED]
- PKI – All desktop/laptop computers procured by DON activities for connection to unclassified network services/NIPRNET must include CAC readers. DON activities must enable cryptographic logon for all eligible populations as specified in the JTF-GNO Communications Tasking Order 06-02, 030440Z FEB 06. POC: [REDACTED] (703) 601-0579, [REDACTED]
- PKE – All DON private web servers must be PK-enabled to allow both server-side and client-side DoD PKI authentication. Website owners should consider implementing additional access controls when additional data segregation and need-to-know requirements are present. DoD PK-enabling requirements and the definition of a private web server can be found in DoD Instruction 8520.2 (PKI and PK-Enabling), viewable at <http://www.dtic.mil/whs/directives/corres/html/85202.htm>. POC: [REDACTED] (703) 601-0579, [REDACTED]
- Privacy – Per Section 208 of the E-Government Act of 2002, DON activities must perform Privacy Impact Assessments (PIA) before developing or procuring IT systems that collect, maintain, or disseminate information in a personally identifiable

Subj: DEPARTMENT OF THE NAVY (DON) INFORMATION TECHNOLOGY (IT)
POLICY GUIDANCE FOR FISCAL YEAR (FY) 2007 EXPENDITURES

form from or about the public. A summary of the E-Government Act, and a link to the text of the Act, may be found at

<http://www.whitehouse.gov/omb/egov/omb/egov/g-4-act.html>. POC: [REDACTED]

[REDACTED] (703) 602-6882, [REDACTED]

- Wireless Technology Security – Wireless devices integrated with or connected to DoD networks are considered to be part of those networks, and must comply with DoD Directive 8500.1 and DoD Instruction 5200.40. (DoD instructions and directives may be viewed at <http://www.dtic.mil/whs/directives/index.html>.) Additionally, for data devices and services, strong authentication, non-repudiation, and personal identification are required for access to a DoD Information System (IS). To ensure consistency of architecture, standards, and security across the DON enterprise, commands are directed to coordinate with their respective DON Deputy CIO, Navy or Marine Corps, prior to expending resources on any infrastructure initiative involving a wireless data solution outside of the existing NMCI solution. Existing wireless installations are required to comply with security regulations and will be addressed on a case-by-case basis. POC: [REDACTED] (703) 601-0230, or [REDACTED]

Questions concerning this guidance, or the Department's business process transformation efforts may be directed to [REDACTED] DON CIO Investment Management Team Lead, at (703) 602-6847, or [REDACTED]



D. M. Wennergren

Distribution:

CNO (N6)
CMC (DCMS, C4)
CHNAVPERS
CNIC
COMUSFLTFORCOM
COMPACFLT
COMUSNAVEUR
COMUSNAVCENT
COMSC
COMNAVRESFORCOM
BUMED
COMNAVVAIRSYSCOM
COMSPAWARSYSCOM
COMNAVFACECOM
NAVPGSCOL

Subj: DEPARTMENT OF THE NAVY (DON) INFORMATION TECHNOLOGY (IT)
POLICY GUIDANCE FOR FISCAL YEAR (FY) 2007 EXPENDITURES

Distribution: (continued)

NAVHISTCEN
COMNAVSUPSYSCOM
FLDSUPPACT
COMNAVSEASYSYSCOM
USNA
NAVWARCOL
COMNAVLEGSVCCOM
ONI
COMNAVSAFCEN
NETC
NAVSTKAIRWARCEN
DIRSSP
COMNAVSPECWARCOM
OPNAVSUPPACT
COMOPTEVFOR
COMNAVSYSMGTACT
COMNAVNETWARCOM

Copy to:

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

GC

CNO (N82)