



DEPARTMENT OF THE NAVY
OFFICE OF THE CHIEF OF NAVAL OPERATIONS
2000 NAVY PENTAGON
WASHINGTON, DC 20350-2000

2000
Ser N6/6U841020
27 Oct 06

From: Deputy Chief of Naval Operations (Communication Networks)
(N6)

Subj: MANDATORY ACTION FOR REDUCING THE NAVY'S INFORMATION
MANAGEMENT (IM)/INFORMATION TECHNOLOGY (IT) FOOTPRINT

Ref: (a) CNO Washington DC 121810Z Sep 06
(b) DON CIO Washington DC 091919Z Aug 06
(c) 10 USC 2222/US Congress 24 Oct 04
(d) USD Washington DC Business Systems Investment Review
Related Guidance of 11 Apr 06
(e) DON CIO Washington DC Information Technology System
Recertification and Registration Guidance Version 2.0
of 19 Dec 05
(f) DON CIO Washington DC 021320Z May 06

1. The Chief of Naval Operations (CNO) has directed OPNAV N6 to take control of the Navy's Information Technology (IT) investments to ensure Navy enterprise-wide IT security, interoperability and return on investment. The end result expected is the Navy will achieve adequate ashore IT asset visibility (cost and configuration) in preparation for post Navy Marine Corps Intranet (NMCI) environment in FY10. In support of reference (a) and the CNO's direction, and in coordination with Department of Navy Chief Information Officer (DON CIO), Financial Management Branch (FMB), Program Executive Office-Enterprise Information Services (PEO-EIS), Deputy Chief of Naval Operation (Integration of Capabilities and Resources (N8)) Naval Network Warfare Command (NETWARCOM), Functional Area Managers (FAMS), and Echelon II commanders, the following guiding principles apply:

a. Applications.

(1) Only Navy Operational Designated Approval Authority (DAA) accredited and Functional Area Manager (FAM) 'Approved' or 'Approved - Interim Waiver' (AIW) applications, as identified in Department of the Navy Application and Database Management System (DADMS), will be allowed to be connected to NMCI and/or OCONUS Navy enterprise-network (ONE-NET). Commanders must

Subj: MANDATORY ACTION FOR REDUCING THE NAVY'S INFORMATION
MANAGEMENT (IM)/INFORMATION TECHNOLOGY (IT) FOOTPRINT

justify the continued use of 'Allowed With Restriction' (AWR) applications by obtaining FAM disposition change to 'AIW' in DADMS.

(2) Commercial Off-The-Shelf (COTS) applications which are no longer supported by the commercial vendor will be disapproved by FAMS. Additionally, Echelon II commands eliminate these COTS application from use.

(3) FAMS shall disapprove Government Off-The-Shelf (GOTS) applications which use a COTS application as a component beyond the vendor's support period. Additionally, Central Design Activities System (CDAS) or application program managers shall maintain version synchronization with COTS versions within their program's configuration management process. GOTS applications with COTS components beyond support period will not be allowed unless specifically approved by my office. My office will only approve GOTS for which the program manager and/or application owner is actively pursuing and resourcing an upgrade to vendor supported COTS applications.

(4) Each Echelon II Commander will justify to the applicable FAM the continued use of applications and/or systems only used by a single command within their scope as identified in DADMS.

(5) No more than two versions of any application and/or system will be used in the Navy unless specifically approved by my office. This action improves security, reduces the costs associated with maintaining multiple applications and promotes interoperability.

(6) Applications and/or systems that have not completed the required Defense Information Technology Security Certification and Accreditation Process (DITSCAP) or Defense Information Assurance Certification and Accreditation Process (DIACAP) per reference (b) and do not have a current Authority To Operate (ATO) or Interim Authority To Operate (IATO) will be eliminated from use in the Navy.

(7) Resources shall not be expended in developing new applications and/or systems without the appropriate FAM approval

Subj: MANDATORY ACTION FOR REDUCING THE NAVY'S INFORMATION
MANAGEMENT (IM)/INFORMATION TECHNOLOGY (IT) FOOTPRINT

documented in DADMS and/or DITPR-DON. Additionally, FAMS shall not approve the development of new applications and/or systems unless they provide a new warfighting or business capability, or will eliminate at least one existing FAM approved or 'AIW' application and/or at least one system identified in DITPR-DON respectively.

(8) A Navy-wide solution must be developed and implemented for each application and/or system which is connected to or implemented on any of the Navy's enterprise networks (NMCI, ONE-NET, and Integrated Shipboard Network System (ISNS)).

b. Systems. Paragraphs 1a(2) through (8) above apply. Additionally, all IM/IT systems must be reported in DITPR-DON and all Defense Business Systems (DBS) must comply fully with the guidance, reporting and certification requirements outlined in references (c) through (f). Any IM/IT system not in compliance with the above will be eliminated from use in the Navy.

c. Servers and Networks.

(1) Server consolidation/elimination and network elimination will be paced by the current Cyber Condition Zebra (CCZ) network shutdown schedule and integrated under legacy network reduction task force scheme of maneuver, commencing in FY07.

(2) Legacy network reduction will expand CCZ, program manager NMCI Legacy Network Shutdown (LNS), and Information Technology Asset Reduction Integrated Project Team (ITAR IPT) efforts to include all CONUS and OCONUS secret and below networks.

(3) Networks without required certification and accreditation or with expired certification and accreditation shall be disconnected from all Navy/DOD networks and action taken to eliminate the network from use.

(4) New and existing network servers shall be employed to maximize efficiencies on a Navy regional and/or enterprise level, vice a local command level.

Subj: MANDATORY ACTION FOR REDUCING THE NAVY'S INFORMATION
MANAGEMENT (IM)/INFORMATION TECHNOLOGY (IT) FOOTPRINT

(5) Echelon II Commander justification for continued operation of an existing network in lieu of an enterprise network (NMCI and/or ONE-NET) is required. The justification that such network supports mission capabilities that are incompatible with NMCI or ONE-NET must be documented in DADMS for each network. Requests will be evaluated and adjudicated with network owners by NETWARCOM and my office.

(6) Retaining networks for support of applications listed in DADMS as 'AWR' is not authorized.



M. J. EDWARDS
Vice Admiral, U.S. Navy

Distribution:

COMFLTFORCOM NORFOLK VA (N00)	CNI WASHINGTON DC (N00)
COMNAVAIRSYSCOM PATUXENT RIVER MD (N00)	USNA ANNAPOLIS MD (N00)
COMNAVSECGRU FT GEORGE G MEADE MD (N00)	OGC WASHINGTON DC (N00)
NAVWARCOL NEWPORT RI (N00)	NAVOBSY WASHINGTON DC (N00)
COMNAVFACECOM WASHINGTON DC (N00)	PEO SHIPS WASHINGTON DC
COMNAVSEASYSYSCOM WASHINGTON DC (N00)	PEO EIS WASHINGTON DC
COMNAVSUPSYSCOM MECHANICSBURG PA (N00)	DIRSSP WASHINGTON DC (N00)
COMSPAWARESYSCOM SAN DIEGO CA (N00)	NAVPGSCOL MONTEREY CA (N00)
CNR ARLINGTON VA (N00)	ONI WASHINGTON DC (N00)
COMPACFLT PEARL HARBOR HI (N00)	NETC PENSACOLA FL (N00)
CDR USJFCOM NORFOLK VA (N00)	BUPERS MILLINGTON TN (N00)
CDR USPACOM HONOLULU HI (N00)	PEO LMW WASHINGTON DC
COMNAVEUR NAPLES IT (N00)	NAVY JAG WASHINGTON DC (N00)
COMUSNAVCENT BAHRAIN BA (N00)	COMOPTEVFOR NORFOLK VA (N00)
PRESINSURV NORFOLK VA (N00)	PEO JSF PATUXENT RIVER MD
COMNAVSPECWARCOM CORONADO CA (N00)	PEO C4I SAN DIEGO CA
COMNAVRESFOR NEW ORLEANS LA (N00)	PEO IWS WASHINGTON DC
NAVHISTCEN WASHINGTON DC (N00)	
CNO WASHINGTON DC (N00, N00N, N09, N1, N2, N4, N40, N402, N6, N8, N091, N093, N095, N097, DNS)	
PEO CARRIERS WASHINGTON DC	
PEO SUB WASHINGTON DC	
FLDSUPPACT WASHINGTON DC (N00)	
PEO TAP PATUXENT RIVER MD	
COMNAVSAFECEN NORFOLK VA (N00)	