DEPARTMENT OF THE NAVY

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

5 December 2011

MEMORANDUM FOR DISTRIBUTION

Subj: DEPARTMENT OF DEFENSE INFORMATION TECHNOLOGY PORTFOLIO REPOSITORY – DEPARTMENT OF THE NAVY (DITPR-DON) PROCESS GUIDANCE (V1.0)

Ref: (a) Department of Defense Information Technology Portfolio Repository – Department of the Navy (DITPR-DON) Registration Guidance for 2006, June 2006

Encl: (1) Department of Defense Information Technology Portfolio Repository – Department of the Navy (DITPR-DON) Process Guidance (v1.0)

Enclosure (1) is the Department of Defense (DoD) Information Technology (IT) Portfolio Repository – Department of the Navy (DITPR-DON) Process Guidance (v1.0), which updates and supersedes reference (a). DITPR-DON is the authoritative source for the Department of the Navy (DON) IT systems and is the data source for multiple internal and external reports and processes. This guidance document provides a comprehensive discussion of core DITPR-DON functionality and basic lifecycle transactions. It will enable users to gain the understanding necessary to perform the basic IT asset management functions of registering, transferring, and archiving DON IT systems within DITPR-DON.

Enclosure (1) may be revised in the future to address changes in core DITPR-DON processes resulting from changes in DoD or DON policies and/or processes.

This guidance is effective immediately. For additional information, please contact Dr. Michelle Schmith, (703) 695-1851, DSN 225, michelle.schmith@navy.mil.

Terry A. Halvorsen

Distribution:
CNO (DNS, N09I, N093, N09S, N097, N1, N2/N6, N3/S, N4, N8)
CMC (ACMC, ARI, M&RA, I, I&L, PP&O, C4, P&R)
ASN (RD&A) – ACQUISITION FAM
ASN (M&RA) – CIVILIAN PERSONNEL FAM
ASN (I&E)
ASN (FM&C) – FINANCIAL MANAGEMENT FAM
GC – LEGAL FAM
DON/AA
DUSN/DCMO

Distribution: (continued)
DUSN (PPOI)
ASN RDA CHSENG
DASN C4I/SPACE
DASN AIR
DASN SHIPS
DASN RDT&E
DON DEP CIO (Navy)
DON DEP CIO (Marine Corps)
COMFLTCYBERCOM Command Information Officer
COMUSFLTFORCOM Command Information Officer
COMUSNAVEUR Command Information Officer
COMPACFLT Command Information Officer
COMUSNAVCENT Command Information Officer
BUMED Command Information Officer
COMNAVDIST Command Information Officer
USNA Command Information Officer
COMNAVAIRSYSCOM Command Information Officer
COMNAVRESFORCOM Command Information Officer
NETC Command Information Officer
COMNAVSEASYSCOM Command Information Officer
COMNAVSUPSYSCOM Command Information Officer
DIRSSP Command Information Officer
CNIC Command Information Officer
NAVPGSCOL Command Information Officer
COMNAVFACENGCOM Command Information Officer
COMNAVSAFECEN Command Information Officer
BUPERS Command Information Officer
COMUSNAVSO Command Information Officer
ONI Command Information Officer
ONR Command Information Officer
COMSPAWARSYSCOM Command Information Officer
NAVHISTHERITAGECOM Command Information Officer
PEO C4I SAN DIEGO CA
PEO CARRIERS WASHINGTON DC
PEO EIS WASHINGTON DC
PEO SPACE SYSTEMS CHANTILLY VA
PEO LAND SYSTEMS QUANTICO VA
PEO IWS WASHINGTON DC
PEO LMW WASHINGTON DC
PEO SHIPS WASHINGTON DC
PEO SUB WASHINGTON DC
PEO ASW ASM PATUXENT RIVER MD

Distribution: (continued)
PEOTACAIR PATUXENT RIVER MD
PEOUAVNSTRKWPNS PATUXENT RIVER
PEO JSF ARLINGTON VA
MARCORSYSCOM
MARFORCYBERCOM

Department of Defense Information Technology Portfolio Repository – Department of the Navy (DITPR-DON)

PROCESS GUIDANCE

Version 1.0

28 November 2011

DEPARTMENT OF THE NAVY
CHIEF INFORMATION OFFICER

DOCUMENT CONTROL CHANGE

Version Number	Date of Issue	Section(s)	Brief Description of Change

CONTENTS

FIGURES

TABLES

APPENDICES

Executive Summary

This *Department of Defense Information Technology Portfolio Repository – Department of the Navy (DITPR-DON) Process Guidance* document provides a comprehensive discussion of core DITPR-DON functionality and basic lifecycle transactions. This information will enable all users to gain the understanding necessary to perform the basic information technology (IT) asset management functions of registering, transferring, and archiving Department of the Navy (DON) IT systems within DITPR-DON. Guidance is also provided on the administrative and user-based roles and responsibilities associated with DITPR-DON, clearly delineating the requirements for each task and step within the core transactions. Specific information on how to access guidance on additional functionality capabilities of DITPR-DON is also provided in this document.

DITPR-DON is the single authoritative source for data regarding IT systems, including National Security Systems (NSS). It provides senior DON decision makers with the context and key information to support IT investment decisions. DITPR-DON also provides consistent automated processes across the Department to meet both internal and external compliance reporting requirements associated with numerous federal and defense policies and mandates. It is imperative that DON users, administrators, and stakeholders understand the critical role that DITPR-DON plays in IT asset management and IT investment management, and its overall value as a tool to support DON IT portfolio management. This guidance document has been published to ensure that a knowledgeable foundation for DITPR-DON use has been established.

Department of Defense Information Technology Portfolio Repository – Department of the Navy (DITPR-DON) Process Guidance

1.0 Introduction

1.1 Purpose

The purpose of this guidance is to give users of the Department of the Defense (DoD) Information Technology (IT) Portfolio Repository – Department of the Navy (DITPR-DON) a foundational understanding of how to perform basic functions to register, transfer to another portfolio, and archive DON IT systems. Also provided are sources for additional information about other functionality.

After reading this document the reader will understand:

- The relationship between DITPR-DON, DADMS, and DoD DITPR,
- What DITPR-DON does and what compliance requirements it supports,
- What roles, responsibilities, and activities are assigned to various stakeholders/users,
- How to gain access to DITPR-DON,
- What should be entered into DITPR-DON and when,
- How to transfer a system another portfolio,
- How to archive and un-archive an IT system, and
- Where to get additional information for DITPR-DON supported processes.

Acronyms and terms used in this guidance are defined in Appendix A.

1.2 Scope

This document focuses on processes behind the core DITPR-DON functionality and basic lifecycle transactions (e.g., system registration, transfer to another portfolio, and archiving). It does not address the many specialized processes (e.g., certification and accreditation, architecture compliance, business system certification and annual review, etc.) as these are addressed by other policies and guidance that change regularly. These documents may be found in the Reference Documents section of DITPR-DON (see Figure 1).

Figure 1: Reference Documents Section in DITPR-DON

1.3 Background

The Department of the Navy Chief Information Officer (DON CIO) memorandum of 18 October 2002 designated the DON Application and Database Management System (DADMS) as the Authoritative Data Source (ADS) for DON IT and NSS applications and database inventory and IT Systems Registration. DADMS is a web-enabled repository of IT applications and systems and their associated data structures and data exchange formats. It supports the DON in the reduction of legacy applications and the development of standard applications, databases, and data elements. It also supports IT interoperability, Information Assurance (IA) assessments, defense business system investment management, and the construction and maintenance of functional and enterprise architectures.

As a result of the "Y2K Initiative," Congress created the IT Registry in order to collect and maintain a repository of all mission critical (MC) and mission essential (ME) systems within the DoD. In 2004, the Government Accountability Office (GAO) provided a report stating that billions of dollars continued to be invested in DoD business systems modernizations with inadequate management oversight and accountability. The DoD IT Portfolio Repository (DITPR) was developed as a result of this audit for the purpose of managing DoD business systems. The

scope of DITPR was expanded to include all DoD IT (including NSS) systems in October 2005 when the IT Registry was merged into DITPR. As a result, DITPR was designated the ADS for all DoD IT systems and, in January 2006, became the official unclassified DoD data source for several major internal and external reports and processes. These include but are not limited to:

- Defense Business System (DBS) development/modernization certifications under the FY2005 National Defense Authorization Act (NDAA),
- Federal Information Security Management Act (FISMA) of 2002,
- DoD-wide inventory of MC and ME systems,
- E-Authentication reporting in compliance with the E-Government Act,
- Privacy Impact Assessment (PIA) compliance,
- Privacy Act (PA) compliance,
- Interoperability certifications,
- Clinger-Cohen Act (CCA) compliance,
- Portfolio Management in accordance with Department of Defense Directive (DoDD) 8115.01, and
- Registry for systems under Department of Defense Instruction (DoDI) 5000.2.

In order to meet the increasing number of reporting requirements of DITPR for IT systems, the DON created a separate and distinct system view within DADMS called the *DoD IT Portfolio Repository-Department of the Navy* (DITPR-DON). DITPR-DON provides the capability to manage IT systems. It is not an independent program; rather it is the "system module" within DADMS. DITPR-DON is now the single, authoritative source for data regarding DON IT systems, including NSS. It also serves as the source for collecting the required IT system data and uploading it to the DITPR. This process is outlined in section 3.4 of this guidance document.

Figure 2 illustrates the distinct modules within DADMS used for the registration of each type of IT asset and the relationship between these modules.

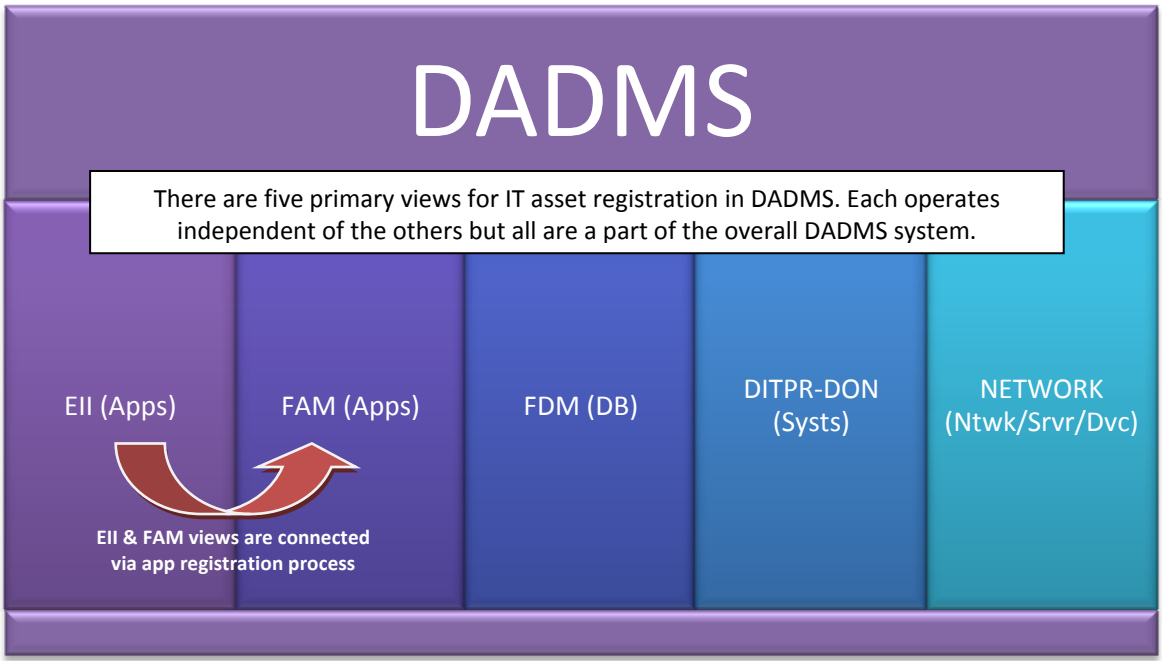

Figure 2: Relationship between DADMS Modules

1.4 DITPR-DON Functionality

DITPR-DON is the system module within DADMS. It contains the DON's authoritative inventory of IT systems. DITPR-DON is accessible to DON users via the Internet, and provides senior DON decision makers with the context and key information to support IT investment decisions. DITPR-DON also provides consistent automated processes across the Department to meet both internal and external compliance reporting requirements associated with:

- Business System Certification Process and annual reports to Congress required by Title 10 United States Code (USC) 2222(g);
- Information Assurance management process and annual reports to Congress in accordance with the Federal Information Security Management Act (FISMA) of 2002;
- DoD-wide inventory of MC and ME systems required by 10 USC 2223(a)(5);
- E-Authentication Report, per Office of Management and Budget (OMB) memorandum M-04-04, December 16, 2003, "E-Authentication Guidance for Federal Agencies," implementing Section 203 of the E-Government Act of 2002, (44 USC Chapter 36);
- Privacy Impact Assessment (PIA) compliance information per OMB Memorandum September 26, 2003, "Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002," II.C.3.a.ii.;
- The Privacy Act of 1974;
- Interoperability certifications required by DODI 4630.8, and CJCSI 6212.01E;
- IT portfolio management, per DODD 8115.01 for all Mission Areas;
- Clinger-Cohen Act registration per DODI 5000.2, E.4.2.4.1 ;
- DON Enterprise Architecture (EA); and
- IT Budget information in Naval Information Technology Exhibits/Standard Reporting (NITE/STAR) memo.

DITPR-DON has many features that support lifecycle and compliance requirements for IT systems. However, this guidance document addresses only the basic IT asset management processes (e.g., registration, transfer, and archiving) that fall within the "system overview" functionality. The other DITPR-DON features described below (items 2, 3, and 4) are not in the scope of this document. Guidance, process, and policy documents for those out of scope features may be found in the Reference Documents section of DITPR-DON (see Figure 1).

1. **System Overview** – DITPR-DON contains foundational information necessary to support all major IT management processes such as: system name, acronym, description, approval authority, points of contact (POC), etc. DITPR-DON also supports the DON Enterprise Architecture process.
2. **System Compliance** – DITPR-DON is a critical tool used to enforce best practices and standard processes to help the Department satisfy compliance and internal/external reporting requirements. This includes regularly scheduled reports driven by legislative or regulatory mandates, annual reports required by other federal departments, and ad hoc reports.

3. **Business System Investment Management** – DITPR-DON includes functionality to support investment management requirements for IT defense business systems (DBS) prescribed by the 2005 NDAA. This functionality includes specialized documentation generation and workflow to track documents submitted through the Business Mission Area (BMA) Investment Review Board (IRB) and the Defense Business Systems Management Committee (DBSMC) for certification of architecture compliance and approval to obligate funds.
4. **Business Enterprise Architecture (BEA) Compliance** – After each major release of the DoD BEA, key architecture products/views (i.e., operational activities, system functions, process steps, and business capabilities) are incorporated into DITPR-DON. This information is used to support BEA compliance assertions and portfolio management activities within the BMA.

Figure 3 below summarizes these features.

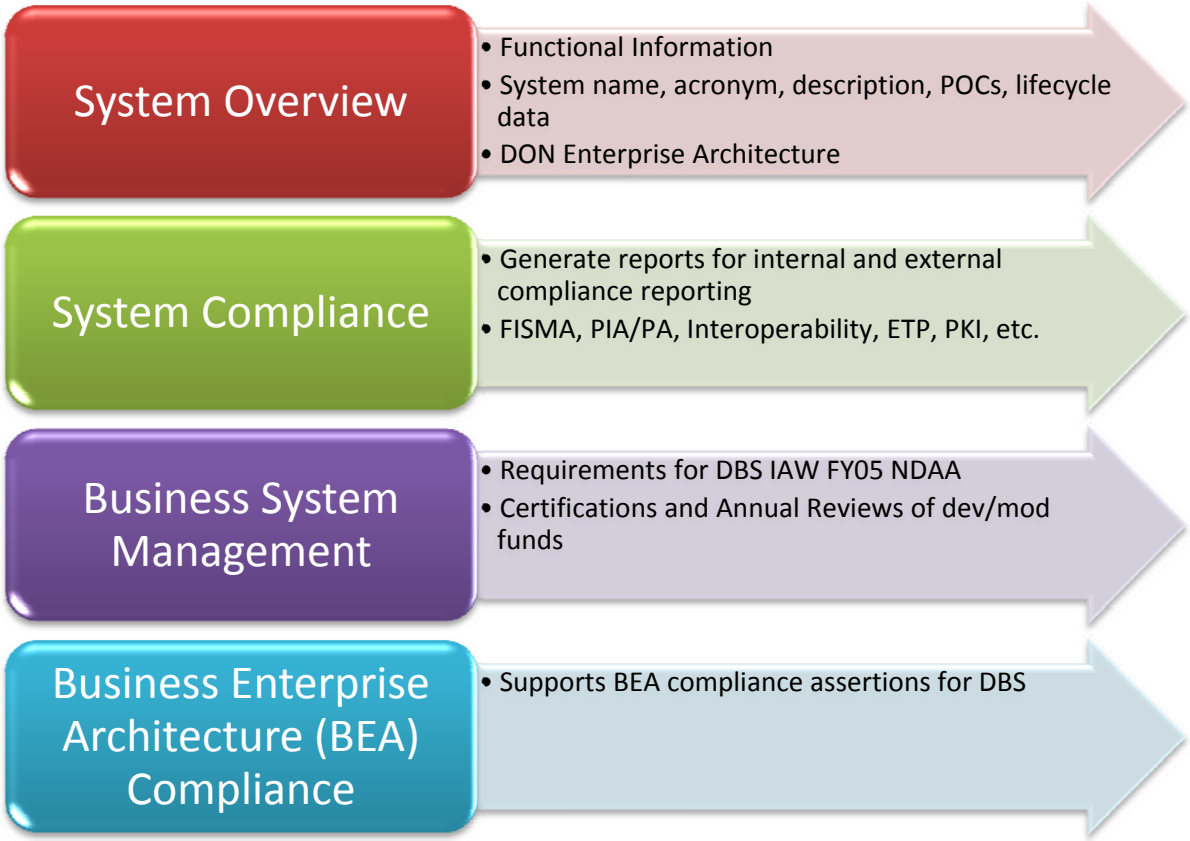

Figure 3: System Information Categories

2.0 DITPR-DON Administration

This section provides guidance on the administrative tasks associated with DITPR-DON. It defines the various roles, responsibilities, and activities of DITPR-DON stakeholders and users and explains how to register for a DITPR-DON account.

2.1 Roles and Responsibilities

To ensure that users have a legitimate need to use DITPR-DON before granting them access, those requesting access to DITPR-DON must have their request endorsed by their supervisor/sponsor (military or civilian (Mil/Civ)) prior to submission. All administrative roles and responsibilities are outlined in Table 1 below.

Table 1: Administrative Roles & Responsibilities

Role	Activities
Account Sponsor (Mil/Civ)	• Confirms need for access by individual(s) requesting a DITPR-DON account • NOTE: Account Sponsor *does not* require a DADMS/DITPR-DON account
Service Administrator (Mil/Civ)	• Applies the appropriate permissions (e.g., view, edit, add) to an approved DITPR-DON account • NOTE: Service Administrator *does* require a DADMS/DITPR-DON account
Assistant Service Administrator (Mil/Civ/Contractor)	• Assists the Service Administrator in approving and applying the appropriate permissions (e.g., view, edit, add) to an approved DITPR-DON account • NOTE: Assistant Service Administrator *does* require DADMS/DITPR-DON account

To provide sufficient controls and protection for the information contained in DITPR-DON, the DON Deputy CIO (Navy and Marine Corps) and the DON Assistant for Administration (DON/AA) must identify a Service Administrator (military or civilian) to serve as the primary liaison between their respective Service or office and the DADMS/DITPR-DON Program Office. Individuals assigned as primary liaison also fulfill other administrative responsibilities, as outlined above and as identified by the DADMS Program Manager. Each DDCIO and DON/AA must provide the name of their Service Administrator to the DADMS/DITPR-DON Program Manager and to the DADMS Help Desk by September 1 of each year or within 30 days if the position becomes vacant.

Permissions and access in DITPR-DON are based on the user type and the roles, responsibilities, and specific activities they are required to perform. These are outlined in Table 2 below.

Table 2: User-Based Roles & Responsibilities

User Type	Roles & Responsibilities	Activities
Program Manager / System Owner	• Responsible for the entry (i.e., addition) and maintenance of system records	• Registers and updates system information • Coordinates submission of new and updated system data with the owning Marine Corps Major Subordinate Command or Navy Echelon II Command Information Officer (IO) and the appropriate Functional Area Manager (FAM) • Reviews/updates system data on a regular basis and in accordance with all DON system review policies • Ensures system is identified in the IT budget in accordance with the Financial Management Regulation, Volume 2B, Chapter 18 and that the applicable Budget Initiative Number (BIN) or BIN Exception Code is recorded in the DITPR-DON record
Functional Area Manager (FAM)	• Provides functional oversight for the portfolio consistent with DoD, DON and ASN strategic goals and objectives • Establishes a complete and accurate FAM taxonomy to which systems will be aligned • Ensures all DITPR-DON entries for their functional area are complete and accurate	• Updates the FAM taxonomy as necessary based upon changes to the functional area as well as inputs received from Marine Corps Major Subordinate Command/Navy Echelon II and below Command IOs • Reviews all systems within their functional area for data accuracy on a regular basis and in accordance with all DON system review policies • Provides reports to Program Managers/System Owners on necessary changes/updates needed to maintain complete and accurate system records • Ensures all IT (including NSS) systems registered in DITPR-DON are identified in the IT budget in accordance with the Financial Management Regulation, Volume 2B, Chapter 18 and that the applicable BIN or BIN Exception Code is recorded in each system's DITPR-DON record

User Type	Roles & Responsibilities	Activities
Marine Corps Major Subordinate Command or Navy Echelon II Command IO IT Registration Point of Contact	• Ensures that new systems are entered correctly and completely • Ensures that all MC, ME and MS systems under the command's auspices have been registered in DITPR-DON in accordance with the system registration requirements per this guidance • Ensures all DDCIO compliance and reporting requirements have been met	• Reviews all systems under the command's purview on a regular basis and in accordance with all DON system review policies • Provides reports to Program Managers/System Owners on necessary changes/updates needed to maintain complete and accurate system records • Ensures all IT (including NSS) systems registered in DITPR-DON are identified in the IT budget in accordance with the Financial Management Regulation, Volume 2B, Chapter 18 and that the applicable BIN or BIN Exception Code is recorded in each system's DITPR-DON record
DDCIO (Navy and Marine Corps) and DON/AA	• Serves as the primary POC for all systems under his/her purview o Directs all data calls, communications, etc. regarding systems under their purview through his/her respective chain of command • Ensures Service data is correct and complete in accordance with the system registration requirements per this guidance • Ensures all DON compliance and reporting requirements have been met	• Regularly reviews and uploads the latest DITPR-DON system data to the DITPR in accordance with the requirements as laid out in this guidance • Reports annually to DON CIO, by memorandum, the status of registration of all MC, ME and Mission Support (MS) systems under his/her purview in DITPR-DON and certifies that information provided therein is accurate and complete o This requirement is outlined in the annual DON IT Fiscal Policy Guidance o The format of this annual certification shall be defined by DON CIO each year. Caveats to the certification and corrective plans of action will be included in a Plan of Action and Milestones for those certification items not complete • Reviews all systems under his/her

User Type	Roles & Responsibilities	Activities
		auspices on a regular basis and in accordance with all DON system review policies • Provides reports to the Program Managers/System Owners on necessary changes/updates needed to maintain complete and accurate system records
DON CIO	• Ensures all Office of the Secretary of Defense (OSD) compliance and reporting requirements have been met	• Promulgates DITPR-DON registration guidance. Updates as necessary • Certifies to the DoD CIO each year that the DITPR-DON data as submitted to the DITPR is accurate and complete • Reviews all systems in accordance with all DON system review policies

2.2 Account Request and Access Authorization Process

DITPR-DON account request and access authorization is a two-step process. First, the requester must obtain a DADMS account, which provides "read" access to DITPR-DON. Once a DADMS account has been established, specialized privileges (e.g., "add", "edit", etc.) for DITPR-DON may be requested. These two steps are summarized below. NOTE: DADMS is a Public Key (PK) enabled web site. Users requesting access must have a valid DoD-issued Public Key Infrastructure (PKI) certificate to access the DADMS web site.

Step 1. Complete and Submit Online DADMS (including DITPR-DON) Access Request

a. The DADMS New User Request form may be found at https://www.dadms.navy.mil. On the left panel of the DADMS Home Page, click DADMS ACCESS REQUEST. The *New User Request* form appears. Ensure all required data fields are filled out. All users, both government and contractor, must provide contact information of a government employee who will serve as account sponsor and will approve the user's request for access to the system. The government sponsor is not required to hold an active DADMS account. Once the *New User Request* form is complete and has been submitted (via the Submit button at bottom of page), the DADMS Help Desk will send an email to the account sponsor requesting approval of the account request. *NOTE: All contractors must download, fill out, and forward to their account sponsor a signed DADMS Non-Disclosure Agreement (NDA). The account sponsor must then sign the same DADMS NDA and send it as an attachment, along with their approval email, to the DADMS Help Desk.* As soon as the DADMS Help Desk receives the approval email from the account sponsor, the DADMS account request will be processed within two business days. There is a HELP button on the

top of the form for online assistance, or the DADMS Help Desk may be contacted by email at DADMS@att.com or by phone at (703) 506-5220.

Step 2. Request Additional DITPR-DON Permissions

a. All new user accounts are established as "Read Only" in all views of DADMS, including DITPR-DON. To obtain edit privileges in DITPR-DON, all users must submit a request through the proper chain of command to their respective DITPR-DON Service Administrator.

i. **Navy:** All user permission requests must be submitted via the user's Echelon I/II Command Information Officer (IO) office.

1. Echelon I FAM users must submit permission requests via their lead FAM POC.
2. Echelon II and below FAM users must submit their permission requests through their Echelon I/II Command IO office.

ii. **Marine Corps:** All user permission requests must be submitted via their lead FAM POC.

iii. **SECNAV:** All user permission requests must be submitted directly to the Service Administrator.

3.0 General Guidelines for Usage

This section provides guidance on the core functions in DITPR-DON. The following subjects are discussed in this section:

- When to register a system;
- What must be registered in DITPR-DON;
- How to transfer a system to another Echelon II, FAM, Service, etc;
- How to upload a DITPR-DON record to DITPR; and
- How to archive and un-archive a system record in DITPR-DON.

3.1 When to Register a System

All systems should be entered into DITPR-DON at the time the program is established. For acquisition category (ACAT) I-IV programs, there are three primary system cases: non-business systems, business systems, and an urgent operational need system. The registration point for non-business systems, for which the Joint Capability Integration and Development System (JCIDS) process is used, generally occurs when the designated oversight body has approved an Initial Capabilities Document (ICD). The registration point for business systems, for which the Business Capability Lifecycle (BCL) process is used, occurs at approval of the business case or the appropriate decision authority has approved the program for implementation. System registration may also occur when a Joint Urgent Operational Need is approved for a joint rapid acquisition through the JCIDS process or when the Service approves a rapid acquisition via their own rapid acquisition process.

All other IT systems and acquisition programs (i.e., non-ACAT programs), as defined in the DoD Financial Management Regulation (FMR) Volume 2B, Chapter 18, June 2007, will be reported in DITPR-DON when funding for the system is obligated (including operations and maintenance and defense working capital fund money).

3.2 What Must be Registered in DITPR-DON

To ensure there is a complete and accurate DON inventory of IT systems (including NSS), all afloat and ashore DON IT systems, initiatives that include IT systems, systems-of-systems (SoS), and family-of-systems (FoS) must be registered in DITPR-DON regardless of cost or funding type (e.g., procurement, modernization, operations and maintenance, working capital). IT programs (i.e., SoS, FoS, and initiatives) must be broken down into their sub-systems; each sub-system must be registered in DITPR-DON in addition to the parent SoS, FoS, or initiative.

DoD policies and doctrine (e.g., DoDD 8500.01E, the JP1-02, and the CNSS 4009) contain different definitions for IT systems and applications. To ensure consistency in registration and reporting, the following definitions for system and application will be used to determine what should be entered into DITPR-DON and subsequently in the Echelon II/FAM modules in DADMS:

- *A system is defined as any solution that requires a combination of two or more interacting, interdependent, and/or interoperable hardware, software, and/or firmware to satisfy a requirement or capability.*
- *An application is defined as any software application that uses an existing operating system software program to provide the user with a specific capability or function that is independent of other "applications." If it is dependent on other applications it becomes a system.*

If an IT asset meets the definition for "system", it should be registered in DITPR-DON. If it meets the definition for "application", it should be registered as such in the Echelon II/FAM modules in DADMS (see Figure 2).

Procedures for entering applications in the Echelon II/FAM modules in DADMS are not covered in this guidance. This information may be found within the Reference Documents section of DADMS, which is accessible from the DADMS Main Menu (see Figure 4). A DADMS account is required to access this information.

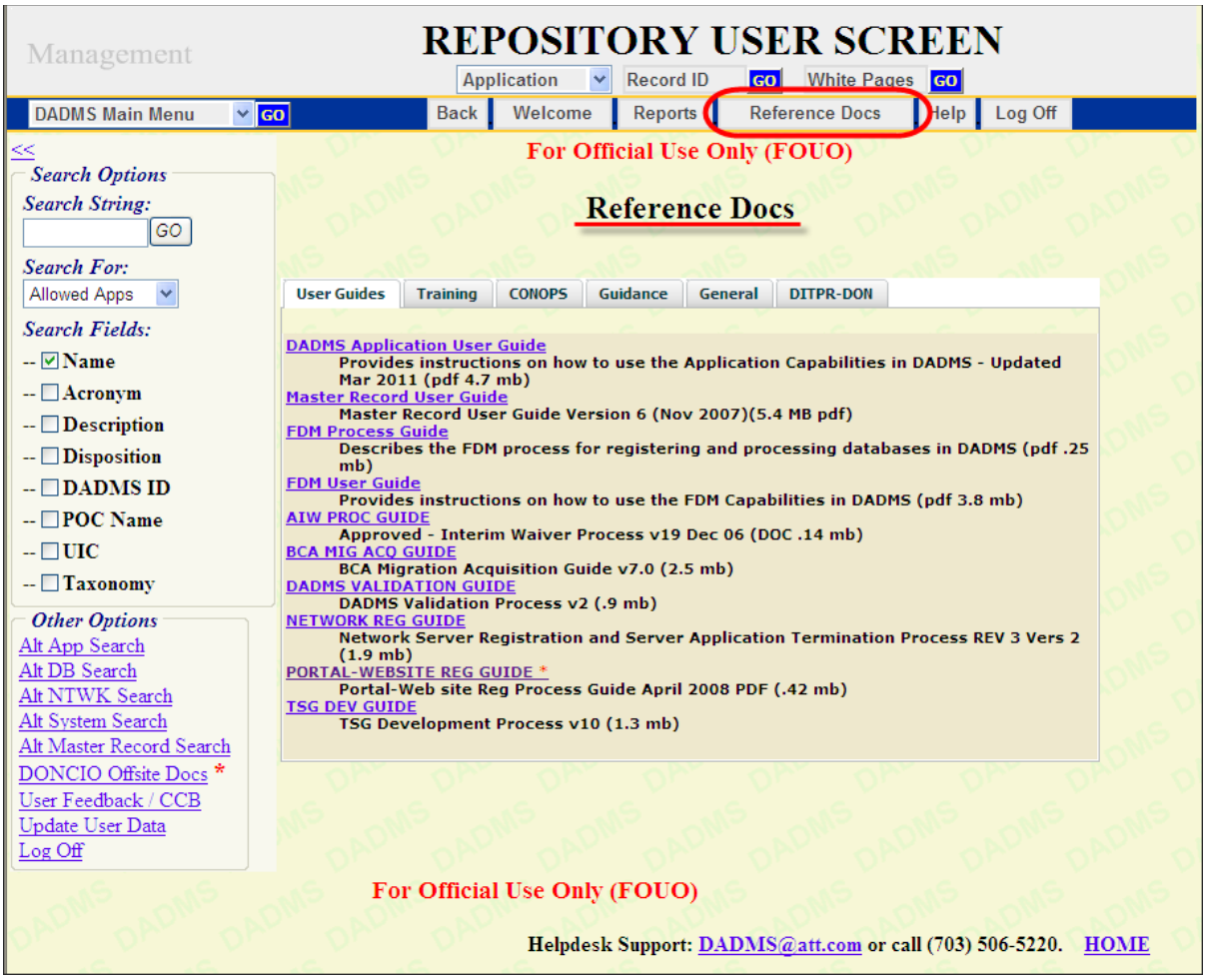

Figure 4: Reference Documents Section in DADMS

3.2.1 Entry Criteria

If an IT asset meets the "system" definition above and satisfies the criteria below, it shall be registered in DITPR-DON.

- Has undergone or is required to undergo IA security accreditation (e.g., DIACAP, etc.) per DoDI 8510.01, *DoD Information Assurance Certification and Accreditation Process* November 28, 2007, Attachment 1 to Enclosure 3, Table E3.A1.T1.
    - **NOTE:** Stand alone systems not connected to a network must undergo IA security accreditation and be entered in DITPR-DON per Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, *Operation of the Joint Capabilities Integration and Development System* (JCIDS) May 11, 2005, and DoDI 8500.2, *Information Assurance Implementation* February 6, 2003.
- Is designated as Platform IT (PIT) in accordance with the DON CIO memorandum 02-10, IA Policy Update for Platform IT policy.

- Is a DBS as defined by Title 10 USC Sec 2222(j)(2) or has a modernization approved by the DBSMC.
- Has been designated as MC or ME system per Title 10 USC 2223(a)(5).
- Is a MS IT system (required by the *2007-2008 DITPR and SIPRNET IT Registration Guidance* August 10, 2009, Appendix C, Paragraph A.3).
- Is a MC or ME system required to undergo Title 40 (formerly CCA) (required per DoDI 5000.02, *Operation of the Defense Acquisition System* December 8, 2008, Enclosure 5, Table 8).
- Is categorized as a NSS, or has been assigned a Mission Assurance Category (MAC) level, or has been designated as a Major Automation Information System (MAIS) (required per the *2007-2008 DITPR and SIPRNET IT Registration Guidance* August 10, 2009, Appendix C, Paragraph A.4).

3.2.2 Registration Guidelines

No data shall be entered into DITPR-DON that would result in the disclosure of classified information. The classification level of information about IT systems is determined by the Marine Corps Major Subordinate Command or Navy Echelon II Command. It is DON policy that all systems including NSS will be registered only **once** in either DITPR-DON or the DoD SIPRNET IT Registry with the following restrictions and exceptions:

- Systems registered in DITPR-DON may be unclassified, sensitive unclassified, CONFIDENTIAL, or SECRET. However, registration data for all systems registered in DITPR-DON shall only include unclassified or sensitive unclassified information.
- Systems registered in the DoD SIPRNET IT Registry may be unclassified, sensitive unclassified, CONFIDENTIAL, or SECRET. However, registration data for all systems registered in the DoD SIPRNET IT Registry shall only include unclassified, sensitive unclassified, CONFIDENTIAL or SECRET information.
- Sensitive Compartmented Information (SCI) and Special Access Program (SAP) systems will be registered in accordance with Intelligence Community registration requirements.
- In the event a system's registration data is collateral TOP SECRET, contact the Marine Corps Major Subordinate Command or Navy Echelon II Command IO office for guidance.

The following additional guidelines and exceptions apply when registering systems in DITPR-DON:

Major Command Designation:

- The Marine Corps Major Subordinate Command or Navy Echelon II Command that is the source of the requirement for the system should be entered as the Major Command in DITPR-DON.
- Exceptions to this rule include but are not limited to the following situations:
    - An Executive Agent (EA) has been named for the system other than the source of the requirement for the system. In this case, the EA shall be responsible for the

registration of and maintenance of the system record and will be entered as the Major Command in DITPR-DON.

- A separate agreement has been made (e.g., Memorandum of Agreement (MOA)) between the source of the requirement for the system and a second party Marine Corps Major Subordinate Command or Navy Echelon II Command, stating that the second party command shall be responsible for the registration of and maintenance of the system record and will be entered as the Major Command in DITPR-DON.

Joint System Registration:

- A joint system is any system used by two or more Military Departments (MilDeps) and/or Defense Agencies. Joint systems are those that have been deployed/implemented under a single IA security accreditation and Title 40 (formerly CCA) confirmation (as applicable) without subsequent modification at any operating Defense Agency or MilDep.
- Marine Corps Major Subordinate Command and Navy Echelon II Commands will register their deployment/implementation of joint systems ***only*** in cases where they are the designated EA of the joint system in order to prevent duplicative reporting in DoD DITPR.
- Variants of Joint Systems:
  - All variants of joint systems used by the Navy and Marine Corps will be registered in DITPR-DON. Variants are considered to exist when:
    - The Marine Corps Major Subordinate Command or Navy Echelon II Command executes its own funding to modify a formal release or version of the joint system to meet its unique requirements; or
    - Rather than implement a new formal release or version of a joint system, the Marine Corps Major Subordinate Command or Navy Echelon II Command decides to retain a former version.
    - All variants of joint systems will be uniquely identified by system name and system acronym:
      - The system name will include both the parent system name and the Marine Corps Major Subordinate Command or Navy Echelon II Command name.
      - The system acronym will include both the parent system acronym and the Marine Corps Major Subordinate Command or Navy Echelon II Command plain language address (PLA).
    - Separate IA security accreditation of a variant is required.

Intra-Departmental System Registration:

- An intra-departmental system is any system used by two or more Marine Corps Major Subordinate Commands and/or Navy Echelon II Commands *within the DON only*. These are systems that have been deployed/implemented under a single IA security accreditation and Title 40 (formerly CCA) confirmation (as applicable) without

subsequent modification at any operating Marine Corps Major Subordinate Command or Navy Echelon II Command.

- Marine Corps Major Subordinate Commands and Navy Echelon II Commands will register their deployment/implementation of intra-departmental systems ***only*** in cases where they are the designated EA of the intra-departmental system in order to prevent duplicative reporting in DoD DITPR.

- Variants of Intra-Departmental Systems:
    - All variants of intra-departmental systems used by Marine Corps Major Subordinate Commands and Navy Echelon II Commands will be registered in DITPR-DON. Variants are considered to exist when:
        - The Marine Corps Major Subordinate Command or Navy Echelon II Command executes its own funding to modify a formal release or version of the intra-departmental system to meet its unique requirements; or
        - Rather than implement a new formal release or version of an intra-departmental system, the Marine Corps Major Subordinate Command or Navy Echelon II Command decides to retain a former version.
        - All variants of intra-departmental systems will be uniquely identified by system name and system acronym:
            - The system name will include both the parent system name and the Marine Corps Major Subordinate Command or Navy Echelon II Command name.
            - The system acronym will include both the parent system acronym and the Marine Corps Major Subordinate Command or Navy Echelon II Command PLA.
        - Separate IA security accreditation of a variant is required.

3.3 How to Transfer Ownership of a System

All system records in DITPR-DON are assigned to portfolios within the DON based on system ownership and the core functionality of the system. Each system is assigned to either the Navy or the Marine Corps as the owning Service. System ownership is further broken down by Echelon II designation. Each system in DITPR-DON is also assigned to a portfolio (i.e., functional area) based on its primary function.

3.3.1 How to Transfer a System to Another Service

Upon initial registration in DITPR-DON, a system is assigned to a Service (i.e., Navy or Marine Corps). **NOTE:** Secretariat systems (i.e., systems managed by DON/AA) are registered under Navy in DITPR-DON. After initial system registration, this assignment is locked and cannot be changed within the system record in DITPR-DON. In order to transfer a system from one Service to another (e.g., change Service designation in DITPR-DON from Navy to Marine Corps), the program manager must manually coordinate the system transfer with and receive written (e.g., memorandum or email) concurrence from both DDCIO (Navy) and DDCIO (Marine Corps) to

ensure that both Services are aware of and agree to the transfer of the system from one Service portfolio to the other. After concurrence has been obtained from both DDCIOs, the PM will:

1. Upload the written concurrence from the current and receiving DDCIOs to the DOC screen of the DITPR-DON system record.
2. Send the transfer request with the written concurrence of the DDCIOs to the DADMS/ DITPR-DON PM for execution of the transfer.

3.3.2 How to Transfer a System to Another Echelon II

The assignment of a Sub-Organization/Echelon II in DITPR-DON may be changed directly within the system record by the program manager. Prior to transferring a system from one Echelon II to another (e.g., change Echelon II from NAVAIR to SPAWAR), the PM must manually coordinate the system transfer with and receive written (e.g., memorandum or email) concurrence from both the Echelon II Command IO for the Echelon II currently listed in the DITPR-DON record and from the Echelon II Command IO for the Echelon II the system is being transferred to. After concurrence has been obtained from both Echelon IIs, the PM will:

1. Upload the written concurrence from the current and receiving Echelon II Command IOs to the DOC screen of the DITPR-DON system record.
2. Change the "Echelon II" data field on the CORE screen in the DITPR-DON system record to reflect the new Echelon II.

NOTE: Once the transfer has been made in DITPR-DON (i.e., the Echelon II field has been changed), the original owning PM and Echelon II will no longer be able to edit the system record. Any changes to the system record, including further transfers of ownership in Echelon II, FAM, etc., must be made by the new owning Echelon II organization.

3.3.3 How to Transfer a System to Another Functional Area Manager

The assignment of a FAM in DITPR-DON may be changed directly within the system record by the PM. Prior to transferring a system from one FAM to another (e.g., change FAM from Logistics to Enterprise Services), the PM must manually coordinate the system transfer with and receive written (e.g., memorandum or email) concurrence from both the FAM currently listed in the DITPR-DON record and the FAM the system is being transferred to. After concurrence has been obtained from both FAMs, the PM will:

1. Upload the written concurrence from the current and receiving FAMs to the DOC screen of the DITPR-DON system record.
2. Change the "FAM" data field on the CORE screen in the DITPR-DON system record to reflect the new FAM.

3.4 How to Upload a DITPR-DON Record to DITPR

After a system has been entered into DITPR-DON it will be uploaded into the DITPR, the ADS for DoD systems information. DITPR-DON and DITPR data is exchanged daily via a web service

interface between the two systems. However, systems registered in DITPR-DON are not *initially* automatically uploaded to DITPR (i.e., first time upload from DITPR-DON to DITPR is not automatic). Title 10 USC Sec 5013 states that the Secretary of the Navy has the authority to equip, train, formulate programs, etc., for the DON. Because of this authority, the Department controls what systems are reported to DITPR and when they are reported.

A system must meet the DITPR-DON upload criteria outlined below in order to be reviewed and marked for upload to DITPR. The designated DDCIO (Navy), DDCIO (Marine Corps), and DON/AA representatives are responsible for reviewing systems that meet upload criteria and marking them for initial upload to DITPR. This review for upload process should occur on a continuous basis to ensure regular and accurate reporting of DON system data to DITPR.

3.4.1 Upload Criteria

In order to maintain the quality of DITPR data, systems that have been registered in DITPR-DON but have not yet been uploaded to DITPR must meet at least one of the following two criteria in order to be flagged in DITPR-DON as "MEETS UPLOAD CRITERIA."

Criteria 1:

- The field "Active/Inactive" is "Active" **and**
- The field "DON Record Type" is "Family of Systems (FoS), System of Systems (SoS), Initiative, or Platform," "System" or "Network"

or

Criteria 2:

- The field "Active/Inactive" is "Active" **and**
- The DITPR-DON entry has been assigned an OSD Budget Identification Number (BIN) or a valid BIN Exception Code. If BIN Exception Code is 9990, the system must have a BIN Explanation in order to receive "MEETS UPLOAD CRITERIA" flag.

3.4.2 Review Process and System Upload to DITPR

Whether the system has ever been uploaded to DITPR in the past determines the process that will be used to upload a record to DITPR. A system must fall into one of the following two categories for its record to be uploaded to DITPR in the daily upload:

1. System record has never been uploaded to DITPR:
    a. System record has been flagged as "MEETS UPLOAD CRITERIA."
    b. System record is individually reviewed, authorized for upload, and marked for export by the designated DDCIO (Navy), DDCIO (Marine Corps), or DON/AA representative.
        i. **NOTE:** Service representatives must check the "System Core Basic" screen of each system prior to marking it off for initial export to DITPR. If a system record has a pink bar at the top of the "System Core Basic" screen indicating either "Missing CORE" or "Missing Trigger" data within the system record (see Figure 5), the request to export the system to DITPR will be rejected by the web service interface schema.

2. System record already exists in DITPR (i.e., previously uploaded to DITPR)
    a. Some or all of the system record has been updated in DITPR-DON since the last daily export of data to DITPR. Only those data fields in the system record that have been updated since the last daily export will be uploaded to DITPR. This upload occurs automatically via the web service interface between DITPR-DON and DITPR (i.e., no manual review and check-off by reviewer is required).

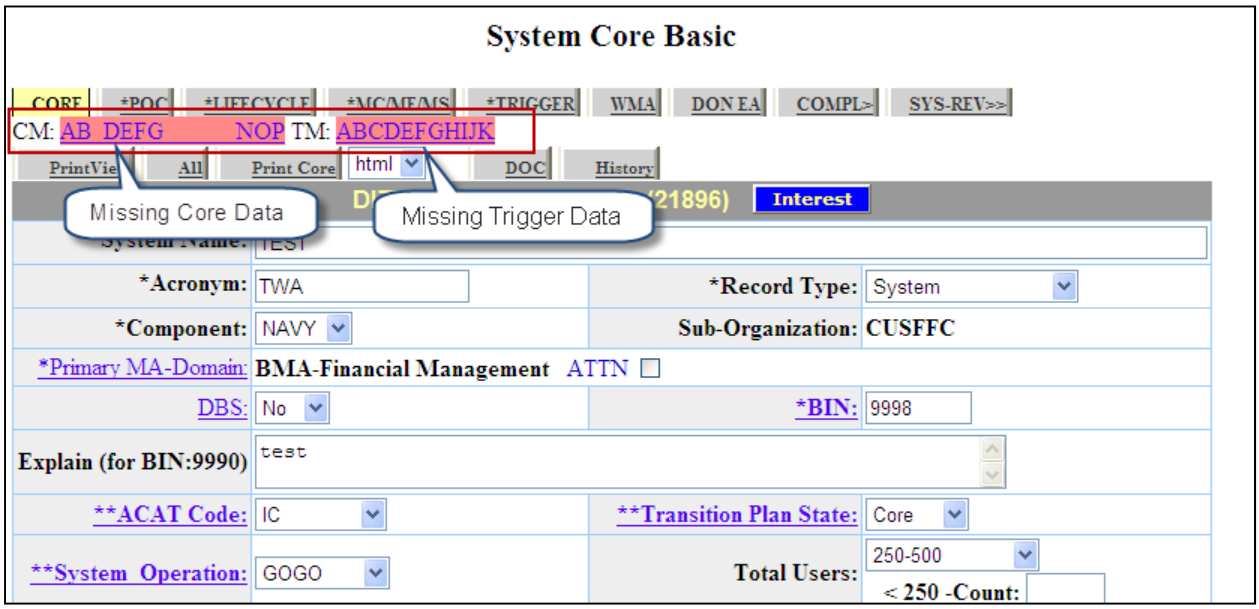

Figure 5: Missing Data Bars on CORE Screen

Review of systems for export to DITPR may take place at any time; however, when there is a high visibility report coming due (e.g., Annual FISMA Report), the DON may implement a hold on marking new systems for initial export to DITPR. The DON will notify the DDCIO (Navy), DDCIO (Marine Corp), and DON/AA representatives charged with reviewing systems for export with the specific time periods when new systems cannot be marked for export.

3.5 How to Archive or Un-Archive a DITPR-DON Record

A system record may only be archived or un-archived by the PM or the owning Navy Echelon II/Marine Corps Major Subordinate Command unless delegation to do so has been authorized and duly noted in writing (e.g., memorandum or email). This written authorization should be uploaded to the DOC screen of the system record. For the purposes of this guidance, it is assumed that the PM will initiate all system archiving or un-archiving.

3.5.1 How to Archive a System Record in DITPR-DON

There are many reasons why a system record may need to be archived. Table 3 outlines the reasons why a system record may be archived in DITPR-DON.

Table 3: Only Valid Reasons for System Archival

Archive Reason	Applicable Conditions
Retirement	• System funding (including all procurement and sustainment funding) is no longer available and/or the project/technology can no longer be supported. • The system is terminated by government direction. • The system is no longer connected to the network, no longer requires security certification and accreditation, *and* is no longer in use.
Replaced	• Record was a placeholder and has been replaced by another entry.
Cancelled	• The system was added to DITPR-DON as a new IT acquisition or an IT development effort and the government decided to cancel the new system or development effort. o This would apply to systems that never reached the deployment stage and would thus not qualify as "retired."
Duplication	• Record was incorrectly added to DITPR-DON twice. • The system's functionality was subsumed (or migrated) into another system. The functionality it provides is no longer required.
Entered in Error	• Record is something that shouldn't have been entered into DITPR-DON to begin with (e.g., application).
Consolidation	• Systems/records have been combined into a single record.

Archiving a system record in DITPR-DON is a two-step process.

Step 1: Determine if Prohibited Conditions Exist. Prior to archiving, ensure no prohibited conditions exist to prevent system archiving in DITPR-DON. Do not archive the system if:

- The system still meets *ANY* DITPR-DON registration requirement.
- The system's lifecycle end date is scheduled after the planned system archive date. This information is found in DITPR-DON under "System Core Basic" and then under the "Lifecycle" tab.
- The system has any current or planned development or modernization. This applies to all systems in all mission areas. This information is found in DITPR-DON under the "Development/Modernization" sub-section of the "Trigger" tab. This section asks

the question: "Current or planned system modernization." If this question is answered "Yes," the system should not be archived.

- The system is a DBS and is currently in the DoD Enterprise Transition Plan (ETP). This information is found in DITPR-DON under "System Compliance" and then under the "ETP" tab.

Step 2: Archive System Record in DITPR-DON. The PM will archive the system record in DITPR-DON. To archive an active system record in DITPR-DON, click the "Change Status" button in the "Active/Inactive" data field on the "System Core Basic" screen in the system record. If any prohibited conditions exist that will not allow the PM to electronically archive the system, these will be noted on the "System Archive" screen. Any such item must be corrected before the system may be archived (see Step 1). If there are no prohibitions, the PM will select the reason for archiving the record (Table 3) and submit.

3.5.2 How to Un-Archive a System Record in DITPR-DON

System records in DITPR-DON should only be archived if they meet one of the acceptable conditions for archival from Table 3, above. If it is determined that a system record has been incorrectly archived (i.e., archived in violation of the business rules and valid reasons for archival), it must be un-archived.

The un-archival of a system record in DITPR-DON is a two-step process.

Step 1: Determine if a Violation of System Archival Has Occurred. Ensure that no prohibited conditions existed at the time of system archival. The system should not have been archived if:

- The system still meetings ***ANY*** DITPR-DON registration requirement.
- The system is still in a developmental or operational lifecycle phase.
- The system still has any funding in the budget and/or is obligating any funding for development, modernization, or operations.

Step 2: Un-Archive System Record in DITPR-DON. If it is determined that the system is still in operation with funds being executed against it, the PM will un-archive the system record in DITPR-DON. To un-archive an inactive system record in DITPR-DON, select the "Active/Inactive Status" drop-down box at the top of the "System Core Basic" screen in the inactive system record. Change the status from "Inactive – …." to "Active – Record" (see Figure 6).

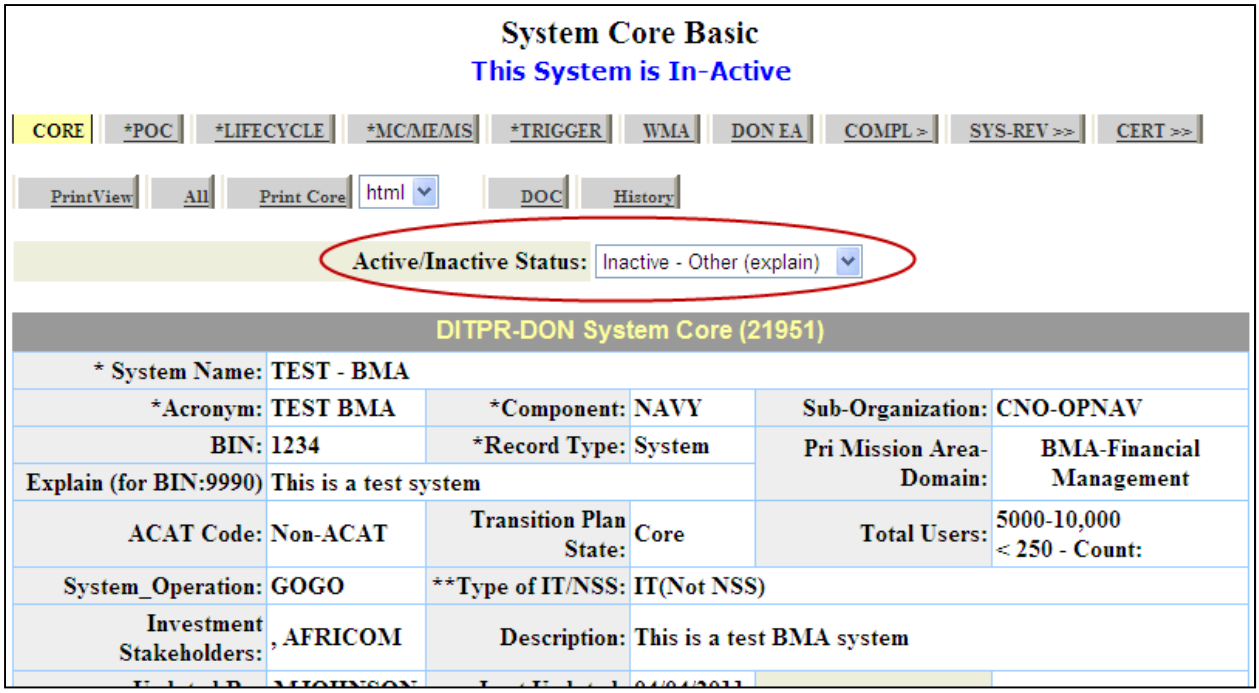

Figure 6: How to Un-Archive a System Record

Appendix A: Glossary of Terms and Acronyms

Term or Acronym	Full Spelling or Definition
Acquisition Category (ACAT)	Categories established to facilitate decentralized decision-making and execution and compliance with statutorily imposed requirements. The ACAT determines the level of review, validation authority, and applicable procedures. Reference d provides the specific definition for each ACAT. (CJCSI 3170.01G)
ADS	Authoritative Data Source
Application	Any software application that uses an existing operating system software program to provide the user with a specific capability or function that is independent of other "applications." If it is dependent on other applications it becomes a system.
C&A	Certification and Accreditation
DADMS	Department of the Navy Application and Database Management System
Defense Business System (DBS)	An information system, other than a national security system, operated by, for, or on behalf of the Department of Defense, including financial systems, mixed systems, financial data feeder systems, and information technology and information assurance infrastructure, used to support business activities, such as acquisition, financial management, logistics, strategic planning and budgeting, installations and environment, and human resource management. (2005 NDAA Sec. 332 § 2222 (j)(2))
DBSMC	Defense Business Systems Management Committee
DDCIO	Department of the Navy Deputy Chief Information Officer
DoD Information Assurance Certification and Accreditation Process (DIACAP)	The DoD process for identifying, implementing, validating, certifying, and managing IA capabilities and services, expressed as IA controls, and authorizing the operation of DoD ISs, including testing in a live environment, in accordance with statutory, Federal, and DoD requirements. (DoDI 8510.01)
DITPR	Department of Defense Information Technology Portfolio Repository
DITPR-DON	Department of Defense Information Technology Portfolio Repository-Department of the Navy
DoD	Department of Defense
DON	Department of the Navy
DON CIO	Department of the Navy Chief Information Officer
FAM	Functional Area Manager

Term or Acronym	Full Spelling or Definition
Family of Systems (FoS)	A set of systems that provide similar capabilities through different approaches to achieve similar or complementary effects. For instance, the warfighter may need the capability to track moving targets. The FoS that provides this capability could include unmanned or manned aerial vehicles with appropriate sensors, a space-based sensor platform or a special operations capability. Each can provide the ability to track moving targets, but with differing characteristics of persistence, accuracy, timeliness, etc. (CJCSI 3170.01F)
Financial Feeder Systems	Financial Feeder Systems are sometimes also referred to as mixed or secondary financial systems. Financial feeder systems are systems that support functions with both financial and non-financial aspects, such as logistics, acquisition, and personnel. They provide key information required in financial processes. For a feeder system, all commands must report the percentage of each feeder system that supports financial requirements. (DoD Financial Management Regulation Volume 2B, Chapter 18, June 2007)
Financial Management Systems	Financial Management systems perform the functions necessary to process or support financial management activities. These systems collect, process, maintain, transmit, and/or report data about financial events or supporting financial planning or budgeting activities. These systems may also accumulate or report cost information, support preparation of financial transactions or financial statements or track financial events and provide information significant to the Agency's financial management. (DoD Financial Management Regulation Volume 2B, Chapter 18, June 2007)
Information Assurance (IA)	Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. (DoDD 8500.1)
Initiative	For DITPR-DON purposes, an initiative refers to the IT Budget definition and usage: "All IT resources will be reported within initiatives. With the exception of Defense business systems (see 180103(G)(2)), initiatives can be systems, programs, projects, organizations, activities or grouping of systems. . . . Group of Systems. With the exception of Defense business systems (see 180102(G)), initiatives can be groupings of systems if all the systems are within the same Mission Area; managed under the same construct, and financed under the same resource construct (program/project/organization)." (DoD Financial Management Regulation Volume 2B, Chapter 18, June 2007)
IRB	Investment Review Board

Term or Acronym	Full Spelling or Definition
Information Technology (IT)	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data or information by the DoD Component. For purposes of the preceding sentence, equipment is used by a DoD Component if the equipment is used by the DoD Component directly or is used by a contractor under a contract with the DoD Component that: E2.1.8.1. Requires the use of such equipment; or E2.1.8.2. Requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term "information technology" includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. Notwithstanding the above, the term "information technology" does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract. (DoDD 8000.1)
Joint	Connotes activities, operations, organizations, etc., in which elements of two or more Military Departments and participate (Joint Publication 1-02)
MilDeps	Military Departments
Mission-Critical (MC) System	A system that meets the definitions of “information system” and “national security system” in the CCA , the loss of which would cause the stoppage of warfighter operations or direct mission support of warfighter operations. (The designation of mission critical shall be made by a Component Head, a Combatant Commander, or their designee. A financial management IT system shall be considered a mission-critical IT system as defined by the Under Secretary of Defense (Comptroller) (USD(C)).) A “Mission-Critical Information Technology System” has the same meaning as a “Mission-Critical Information System.” (DoDI 5000.2, December 8, 2008)
Mission-Essential (ME) System	A system that meets the definition of “information system” in [the CCA], that the acquiring Component Head or designee determines is basic and necessary for the accomplishment of the organizational mission. (The designation of mission-essential shall be made by a Component Head, a Combatant Commander, or their designee. A financial management IT system shall be considered a mission-essential IT system as defined by the USD(C).) A “Mission-Essential Information Technology System” has the same meaning as a “Mission- Essential Information System.” (DoDI 5000.2, December 8, 2008)
Mission-Support (MS) System	A system (as defined in this appendix) that is neither Mission Critical nor Mission Essential.

Term or Acronym	Full Spelling or Definition
National Security System (NSS)	(A) The term "national security system" means any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency – i) the function, operation, or use of which – (I) involves intelligence activities; (II) involves cryptologic activities related to national security; (III) involves command and control of military forces; (IV) involves equipment that is an integral part of a weapon or weapons system; or (V) subject to subparagraph (B), is critical to the direct fulfillment of military or intelligence missions; or (ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy. (B) Subparagraph (A)(i)(V) does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications). (44 USC 3542(b)(2))
NDAA	National Defense Authorization Act
NITE/STAR	Naval Information Technology Exhibits/Standard Reporting; This is the DON's authoritative data source (ADS) for IT budget reporting.
OSD	Office of the Secretary of Defense
Platform Information Technology (PIT)	1. REFERS TO: 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. PIT does not include general purpose systems. 2. MAY: a. Reside aboard or on a platform b. Be stand-alone c. Have an interconnection to other Platform IT (known as a "Platform IT-to-Platform IT Interconnection") d. Have a Platform IT Interconnection (see DoDI 8500.1) to other IT that is not Platform IT (e.g., a general-use ship's network, such as ISNS, or a non-Platform IT system) (Derived from DoDD 8500.1, Paragraph E2.1.16.4)
PM	Program Manager
Portal	Portal is a term, generally synonymous with gateway, for a World Wide Web site that is or proposes to be a major starting site for users when they get connected to the Web or that users tend to visit as an anchor site. Portals provide a way for enterprises to provide a consistent look and feel with access control and procedures for multiple applications and databases, which otherwise would have been different entities altogether. Examples of public web portals are AOL, iGoogle, MSNBC, Netvibes, and Yahoo!.

Term or Acronym	Full Spelling or Definition
Stand-Alone System	A system operating independently of and without interconnection to any other information system. (DoDI 8510.01)
System	Any solution that requires a combination of two or more interacting, interdependent, and/or interoperable hardware, software, and/or firmware to satisfy a requirement or capability.
System of Systems (SoS)	A set or arrangement of interdependent systems that are related or connected to provide a given capability. The loss of any part of the system could significantly degrade the performance or capabilities of the whole. The development of a SoS solution will involve trade space between the systems as well as within an individual system performance. (CJCSI 3170.01F)
Variant	A variant occurs when (1) the Marine Corps or Navy Echelon II command executes its own funding to modify a formal release or version of the joint system/initiative to meet its unique requirements; or (2) rather than implement a new formal release or version of a joint system/initiative, the Marine Corps or Navy Echelon II command decides to retain a former version. Variants require separate IA security accreditation and information entered should uniquely identify the system.
Web Services	Web services provide a standard means of interoperating between different software applications, running on a variety of platforms and/or frameworks. Web services are characterized by their great interoperability and extensibility, as well as their machine processable descriptions thanks to the use of XML. They can be combined in a loosely coupled way in order to achieve complex operations. Programs providing simple services can interact with each other in order to deliver sophisticated added-value services. (World Wide Web Consortium, http://www.w3.org/2002/ws/Activity)