DEPARTMENT OF THE NAVY
BUREAU OF NAVAL PERSONNEL
5720 INTEGRITY DRIVE
MILLINGTON, TN 38055-0000

BUPERSINST 5210.8
BUPERS-01
22 JUN 2011

BUPERS INSTRUCTION 5210.8

From: Chief of Naval Personnel

Subj: IMPLEMENTATION OF THE TOTAL RECORDS INFORMATION MANAGEMENT APPLICATION AS THE ELECTRONIC RECORDS MANAGEMENT SOLUTION WITHIN THE BUREAU OF NAVAL PERSONNEL

Ref: (a) OPNAVINST 5210.20
(b) BUPERSNOTE 5210 of 4 Oct 2010
(c) SECNAV M-5210.1 of Nov 2007

Encl: (1) BUPERS TRIM Context Business Rules and Best Practices Guide (Version 1.0)

1. Purpose. To provide guidance for the implementation of the Total Records Information Management (TRIM) application as the Electronic Records Management (ERM) solution for the storage of electronic records within the Bureau of Naval Personnel (BUPERS).

2. Applicability. This instruction applies to BUPERS Millington, Navy Personnel Command, Navy Recruiting Command, and Navy Manpower Analysis Center.

3. Background. Reference (a) issues Department of the Navy (DON) Records Management Program policies to ensure consistent records management practices within all Office of the Chief of Naval Operations activities. All BUPERS activities shall strictly adhere to guidance contained therein. Reference (b) provides a TRIM implementation and training schedule for BUPERS Millington and Navy Personnel Command (NAVPERSCOM).

4. Electronic Records. A significant and ever increasing portion of command records are created, used, and stored electronically. These records must be managed as stringently as records in any other medium. Electronic records include information that may be recorded on any medium capable of being read by a computer and which satisfies the definition of a record. E-mail records comprise a significant subset of electronic records that need to be appropriately created, maintained, used, and disposed. Not all e-mail messages and other electronically generated information are considered

records. E-mail messages, documents, and files are considered records only when they meet the definition of "Federal records."

b. Filing Procedures for Electronic Records. The DON mandated ERM solution is Tower Software's TRIM Context, which is provided as part of the Navy and Marine Corps Intranet (NMCI) initiative. The software and server platforms are provided for under NMCI; however, the contents and management of those contents are the responsibility of the individual content owners.

(1) Use only approved ERM applications for filing electronic records. Activities with access to the NMCI network will use the TRIM Context program. TRIM is the DON standard for storage of electronic records including e-mail. The BUPERS TRIM dataset has been deployed at the echelon 2 level and is being implemented throughout the rest of the BUPERS activities. Once TRIM is deployed at an activity, its use is required to properly categorize records by standard subject identification code (SSIC) and to file and manage them until final disposition. A file plan is required for records stored in TRIM. Electronic records stored in other Navy enterprise-wide programs, e.g., the Electronic Military Personnel Records System, etc., are exempt from the requirement to use TRIM.

(2) Until TRIM is fully deployed and operational within the activities, records may be maintained in an electronic format or, if deleted from the electronic system, must be printed and filed in the activity's hardcopy filing system pending final disposition. In all cases the permanent deletion of electronic records when not printed and filed must meet the disposition guidance contained in reference (c), part III.

(3) Electronic Records not Stored in TRIM. Electronic records may not be stored in a manner that does not meet the requirements of reference (a). Requests to store electronic records in a system other than TRIM or another approved Navy enterprise-wide program must be submitted in writing to the BUPERS Records Manager (RM) for review.

5. Responsibilities

a. BUPERS

(1) Appoint a BUPERS RM to lead the implementation and monitor the DON Records Management Program within BUPERS.

(2) Appoint a dataset records manager (DRM) to maintain final authority over the BUPERS TRIM dataset for electronic management of records.

b. BUPERS Office of Legal Counsel and Navy Personnel Command (NAVPERSCOM) Office of Legal Counsel

(1) Provide legal assistance to BUPERS headquarters staff and advice to subordinate commands on the proper response to judicial correspondence and or amendments to records, motions for discovery, preservation orders, or other legal actions or issues pertaining to BUPERS electronically managed records.

(2) Provide technical assistance to the BUPERS RM or DRM to ensure BUPERS complies with the electronic Freedom of Information Act requirements and Personally Identifiable Information instructions.

c. BUPERS Security Manager. The BUPERS Security Manager (BUPERS-00Y) will provide technical support for issues pertaining to the proper classification and management of classified records.

d. BUPERS RM

(1) Coordinate with the BUPERS DRM to acquire sufficient TRIM storage space for centralized electronic records management for BUPERS records.

(2) Ensure system administrators include records management plans and procedures that comply with National Archives and Records Administration (NARA) in all configuration management.

(3) Review and make a final determination on requests to store electronic records in any system other than TRIM or other Navy enterprise-wide program.

(4) Review and update this instruction, as required.

e. BUPERS DRM

(1) Customize the generic core configuration in TRIM to effectively reflect the organization's structure.

(2) Set TRIM usage policy and maintain final authority over the organization's TRIM dataset.

(3) Control access to and use of records in the BUPERS TRIM dataset.

(4) Monitor and troubleshoot BUPERS' TRIM dataset.

(5) Develop and maintain business rules for use of BUPERS' TRIM dataset.

(6) Represent the organization's interest through active participation in the TRIM Configuration Board.

f. Dataset Administrator

(1) Trains RMs, command or local administrators, and end user in all facets of TRIM applications.

(2) Implements BUPERS RM and BUPERS DRM policies. Follow all written guidance.

(3) Develops and updates dataset business rules and best practice guide.

(4) Grants access to command or local administrators and oversees access control for BUPERS dataset.

g. Commands

(1) Implement TRIM as the ERM solution for records management using enclosure (1) as a guide.

(2) Appoint in writing a command RM and provide copy of appointment letter and contact information, and any subsequent changes, to the BUPERS RM.

(3) Appoint in writing a command TRIM administrator and local TRIM administrators, as required, to help manage TRIM implementation and sustainment.

h. Command RM

(1) Lead TRIM implementation throughout their command.

(2) Ensure all electronic records are maintained per this and other relevant instructions, regulations, and laws.

i. Command or Local Administrators. Command and local administrators are responsible for controlling all aspects of TRIM within their command or departments, as well as implementing the policies put in place by the BUPERS DRM and command RM. Command or local TRIM administrators will:

(1) Contact the BUPERS DRM to establish the high-level command structure in TRIM and have access granted to the administrator before a command can access the BUPERS TRIM dataset;

(2) Provide training and serve as first line of support to end users within the command or departments;

(3) Ensure all TRIM folders and documents in their area of responsibility have appropriate disposition schedules, SSICs and security applied to them;

(4) Create workflows for sections as needed;

(5) Provide access to TRIM for new employees;

(6) Remove TRIM access to employees who transfer, retire, etc.; and

(7) See enclosure (1) for additional tasks and guidance.

j. End Users. End users will add, retrieve, search, and view records in TRIM. It is the responsibility of end users to understand the definition of a record and appropriately add records to the command dataset when required.

6. Training. Command RMs, command and local administrators, and TRIM end users are required to complete the following training courses:

a. End Users shall complete the following:

(1) Records Management in the DON: Everyone's Responsibility (DOR-RM-010);

(2) TRIM Context via the NMCI (Entry): (DOR-TRIM-101);

(3) BUPERS End User Training Course NPC-TRIMENDUSER: Four hour session (Highly recommended not required); and

(4) TRIM Context via the NMCI (Advanced) (DOR-TRIM-201).

b. Records Manager and Command or Local Administrators:

(1) Will complete all end user training requirements;

(2) DON Records Management: Advanced Topics (DOR-RM-020); and

(3) Local Administrator Course NPC-TRIMADMIN: Two day NAVPERSCOM course.

7. TRIM Help Documents. In addition to the training and guidance in enclosure (1), there are several TRIM help documents in the BUPERS TRIM dataset. These documents are listed in the folder named TRIM Training Manual, in the box labeled TRIM Supporting Documents, which is under the command box HQ. A title word search in TRIM for the word "TRIM Supporting" or "TRIM Course" will also display the TRIM Training Manual folder.

8. Points of Contact. Bureau of Naval Personnel (BUPERS) Data Set Records Manager, at (901) 874-3054 or DSN 882, BUPERS Records Manager at (901) 874-3059 or DSN 882, BUPERS Dataset

System Administrator at (901) 874-3560 or DSN 882, and TRIM Server Administration at 866-843-6624.

D. P. QUINN
Rear Admiral, U.S. Navy
Deputy Chief of Naval Personnel

Distribution
Electronic only, via BUPERS Web site
http://www.npc.navy.mil

BUREAU OF NAVAL PERSONNEL
TRIM Context
Business Rules and Best Practices Guide

VERSION 1.0

JUN 2011

TABLE OF CONTENTS

PARAGRAPH	TITLE	PAGE NUMBER
1.	**POLICY AND USE**	**1**
1.1.	Mandates and Instructions	1
1.2.	Accountability and Obligation	1
1.3.	Requirements Compliance	2
2.0.	**PURPOSE AND ROLES**	**4**
2.1.	Overview	5
2.2	Roles and Responsibilities	6
2.3	System Architecture	7
3.	**DATASET ADMINISTRATION**	**8**
3.1.	BUPERS Dataset Configuration	8
3.2	Standard Dataset Configuration Settings	11
4.	**BUSINESS RULES**	
4.1.	Locations (Person, Positions, Organizations, Teams)	12
4.2	Title and Naming Convention	12
4.3.	Records and Documents Storage	13
4.4.	Security and Access	14
4.5.	Workflows	14
5.	**BEST PRACTICES**	**15**
5.1	Locations (Person, Positions, Organizations, Teams	15
5.2	Title and Naming Convention Folders/Records	15
5.3	Records and Documents Storage	15
APPENDIX		
A	**TRIM QUICK REFERENCE GUIDE**	**A-1**
B	**GLOSSARY OF TERMS**	**B-1**

1. POLICY AND USE

1.1. Mandates and Instructions

a. Per reference (a), all Office of the Chief of Naval Operations activities shall establish a records management program to maintain records consistent with the guidance in the instruction.

b. Per reference (a), all commands on NMCI network must use the provided Department of the Navy (DON) Electronic Records Management System (ERMS) for the storage and management of electronic records.

c. Total Records and Information Management (TRIM) is one of the leading ERM applications and has been chosen for the DON Records Management (RM) Program. TRIM is available on every NMCI seat. The Navy Records Management Program is the largest implementation of TRIM in the world with over 350,000 seats.

d. Reference (a) directed commands to identify a Dataset Records Manager (DRM) for the TRIM dataset implementation.

e. TRIM meets Federal, Department of Defense (DoD), and DON obligations to comply with the mandated records management program. TRIM is DoD 5015.2-STD of 25 April 2007 compliant, DoD Functional Area Manager Approved, and approved for use by the National Archives and Records Administration.

1.2. Accountability and Obligation

a. DON employees have three basic obligations regarding Federal records:

(1) Create records needed to do the business of their agency, record decisions and actions taken, and document activities for which they are responsible;

(2) Maintain records so that information can be found when needed. This means setting up good directories and files, and filing materials (in whatever format) regularly and carefully in a manner that allows them to be safely stored and efficiently retrieved when necessary; and

(3) Dispose of records under their control per DON records schedules and Federal regulations.

b. Federal law requires the DON to maintain an active records management program that provides for the accurate and efficient tracking and retrieval of command records. Command records shall adequately document the organization, operations, functions, policies, procedures, decisions, and transactions of the DON at all levels and provide information necessary to protect the legal and financial rights of persons, commands, and the government. The Navy Records Management Program is designed to ensure records are maintained and disposed of per reference (a) and its references.

c. Concealment, Removal, or Mutilation of Records (18 U.S.C. § 2071). Whoever willfully and unlawfully conceals, removes, mutilates, obliterates, or destroys, or attempts to do so, or, with intent to do so takes and carries away any record, proceeding, map, book, paper, document, or other thing, filed or deposited with any clerk or officer of any court of the United States, or in any public office, or with any judicial or public officer of the United States, shall be fined under this title or imprisoned not more than 3 years, or both.

1.3. Requirements Compliance

1.3.1. Satisfies DON ERMS Requirements. What is a record?

Item	Record?
Records documenting any Navy mission-related activities (program records)	Yes
Records documenting routine Navy housekeeping support activities (administrative records)	Yes
Documents not connected to transactions of agency business	No
Any transactions related to agency business	Yes
E-mail	Yes; except personal content
Active "working files" that document work being done by an Action Officer	Yes; but, working copies may often be destroyed after final document is published

Item	Record?
Extra copies of documents, stocks of publications, library and museum material	No

1.3.2. Satisfies DON Legal Requirements for Records Management

a. Preserves records that contain adequate and proper documentation of the organization, functions, policies, decisions, procedures, and essential transactions of the agency and designed to furnish the information necessary to protect the legal and financial rights of the Government and of persons directly affected by the agency's activities (44 U.S.C. 3101).

b. Establishes safeguards against the removal or loss of records and making requirements and penalties known to agency officials and employees (44 U.S.C. 3105).

1.3.3. Satisfies DON Policy Requirement

a. Ensures electronic records (including e-mail) are scheduled for retention or periodic destruction per reference (c).

b. Reference (c) contains records disposition guidance:

(1) Applies to classified and unclassified records.

(2) Disposition depends on SSIC number; SSIC depends on subject and content of record.

(3) Disposition can range from 3 months to permanent; the majority are to be destroyed within 2 years.

IMPORTANT: With the exception of permanent, official records are **not** to be held indefinitely. Due to policy, legal, and business concerns; records are to be destroyed when eligible to do so.

1.3.4. Supports the efficient and effective retrieval of information

a. Facilitates sharing of information, better access to information means better decision-making.

b. Eliminates unnecessary duplication of information and effort.

c. Minimizes the number and volume of outdated records, while increasing the significance of those to be preserved.

d. Reduces the costs associated with retaining unnecessary information.

e. Increases business efficiencies due to process automation, workflow, and repeatability

2. PURPOSE AND ROLES

a. The objective of this guide is to assist the Bureau of Naval Personnel (BUPERS) Records Managers, Administrators and End Users with the business rules and best practices associated with the implementation of TRIM across BUPERS. The goal of this guide is to provide the workforce with methods of how to electronically manage, store, retrieve, and archive records within the BUPERS TRIM dataset efficiently and effectively. This guide also helps to ensure that BUPERS command or local administrators and records managers (RMs) perform consistent document management practices across the command as well as maintain records and or documents in a secure environment.

b. This guide is not designed as a stand-alone user manual for TRIM. Users are encouraged to reference the TRIM online User Guide, which is available via "Start > Programs > TRIM Context > TRIM User Guide." Additional reference guides and training documents are available in the BUPERS TRIM dataset, and can be found by conducting a Title Word search on the words "**TRIM Supporting Documents**" or record number search for BP-UNT-38. See appendix A for a list of supplemental quick reference guides for standard user functions. Appendix B provides a glossary of terms used throughout this instruction.

Record Number	Title
BP-UNT-38	TRIM Supporting Documents
BP-SEC-11-70	TRIM Course Training Materials
BP-SEC-11-37	TRIM Help Documents / Quick Reference Guides
BP-SEC-10-56	TRIM Briefs
BP-SEC-10-32	Governing Documents

Illustration A - dataset help and training documents

2.1. Overview

2.1.1. Background. TRIM Context is provided as part of the NMCI initiative. The TRIM software, infrastructure and server platforms are provided for under NMCI; however, the contents and management of that data is the responsibility of the data owners, administrators and end users.

2.1.2. Audience. This guide is intended for all personnel who create, manage and dispose of electronic documents and records within BUPERS Dataset.

2.1.3. Definitions

a. End User - this term refers to all users who are not local administrators or the dataset records manager (DRM).

b. Best Practice - represents the recommended command-wide practice for a particular action or functionality.

c. Business Rule - requirement that must be followed and adhered to across the command to ensure consistency and safety of information.

d. Dataset Records Manager (DRM) - person(s) identified to serve as the DRM for the BUPERS dataset.

e. Command or Local Administrator - person identified to serve as a TRIM administrator for their respective command, code, department, or division.

f. Locations - generally refer to organizations, positions, and individuals within the organization. Can also be working groups or project teams.

g. Records - includes all books, papers, maps, photographs, machine readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations or other activities of the Government or because of the informational value of the data in them (44 U.S.C. 3301).

h. Record Type - provides hierarchical structure as a organized means for categorizing data. Most of the record types in TRIM are pre-defined by the DON "Core Configuration" but others can be built and customized to capture specific metadata as deemed necessary by the DRM.

i. Dataset Administrator or Trainer - person(s) identified to serve as the dataset TRIM administrator. This person also provides instructor-led training to end users and administrators as well as over-the-shoulder and ad-hoc support to all BUPERS dataset end-users.

j. TRIM Desktop - the instance of the TRIM application used by end-users

k. TRIM Context - the instance of the TRIM application used by local administrators and the DRM.

2.2. Roles and Responsibilities

2.2.1. Command or Local Administrators

a. The command or local administrator will ensure each end user:

(1) Understands how to select the BUPERS dataset upon login and set it as the default.

(2) Has a profile that is correctly configured.

(3) Is assigned to a unique Location (position, group, department, etc.)

(4) Has the appropriate profile settings, security and access rights.

(5) Integrates TRIM with Microsoft Outlook.

(6) Can navigate successfully to their section's folders or records.

(7) Has "Favorites" established for quickly retrieving their records or activities due.

b. Additionally, command and local administrators will:

(1) Create workflow templates for automation of their standard business processes;

(2) Test the access rights assigned to containers and records to ensure that the proper security and access controls have been correctly applied;

(3) Coordinate with other local administrators when employees transfer departments and have to be re-assigned to a different organization; and

(4) Ensure end-user accounts and access rights are deactivated for all employees leaving or transferring from the command (see Business Rule 4.2.2).

2.3. System Architecture

2.3.1. Network and Dataset. TRIM is a client-server commercial off-the-shelf software owned by Hewlett Packard available on the NMCI network. The name of the BUPERS dataset is Bureau of Naval Personnel.

2.3.2 Hardware. Requirements depending on the geographic location of the user, the appropriate TRIM Workgroup Server name should appear in the "Or TRIM Workgroup Server" field. Users should connect to the Jacksonville, FL Primary TRIM Workgroup Server and should also add a secondary server by going to File > Open Dataset and clicking on Properties and typing in the Secondary Server name:

Jacksonville, FL Servers:
eermJAXStw61.nmci.navy.mil
eermJAXStw62.nmci.navy.mil

Norfolk, VA Servers:
eermNRFKtw61.nmci.navy.mil
eermNRFKtw62.nmci.navy.mil

Pearl Harbor, HI Servers:
eermPRLHtw61.nmci.navy.mil
eermPRLHtw62.nmci.navy.mil

Washington Navy Yard Servers:
eermWNYDtw61.nmci.navy.mil
eermWNYDtw62.nmci.navy.mil

San Diego, CA Servers:
eermSDNItw61.nmci.navy.mil
eermSDNItw62.nmci.navy.mil

3. DATASET ADMINISTRATION

3.1. BUPERS Dataset Configuration

3.1.1. Container Business Rules

Boxes: Command, Sub-Command, and Unit:

No documents can be placed at these levels.

Must follow the command's high-level organizational structure.

Only dataset administrators can change access controls.

Viewable to everyone (the boxes themselves, not necessarily the content within.)

Folders:

a. Section folders can be created by anyone in the dataset but the creator must verify with the command or local administrators that they are set up correctly (security and access controls)

b. Sub-section folders inherit the properties of the section folders they are created under. Administrators must ensure the proper access controls are applied.

c. Teal Folders are the next level followed by the magenta folder, which is the lowest folder level available.

d. Retention schedules are applied at the lowest level where the documents will be stored. This folder is typically titled as a fiscal or calendar year folder, e.g., "PERS-5 CY2010 Correspondence."

Record Number	Title
BP-CMD-1	BUREAU OF NAVAL PERSONNEL - MILLINGTON (BPM) (BUPERS)
BP-CMD-2	NAVY PERSONNEL COMMAND (NPC)
BP-CMD-4	Navy Manpower Analysis Center (NAVMAC)
BP-CMD-5	Commander Navy Recruiting Command (CNRC)
BP-CMD-7	Human Performance Center (HPC)
BP-CMD-9	BPM/NPC MILLINGTON CAMPUS RESOURCES

Illustration B - Command Boxes

Record Number	Title
BP-CMD-1	BUREAU OF NAVAL PERSONNEL - MILLINGTON (BPM) (BUPERS)
BP-SCB-41	MILITARY COMMUNITY MANAGEMENT (BUPERS-3)
BP-SCB-40	PAY & PERSONNEL MANAGEMENT (BUPERS-26)
BP-SCB-36	PRODUCTION MANAGEMENT OFFICE (PMO) (00C2)
BP-SCB-15	ENTERPRISE LIAISON (BUPERS-00EL)
BP-SCB-16	INSPECTOR GENERAL (BUPERS-00IG)
BP-SCB-10	NAVAL PERSONNEL RESEARCH (BUPERS-1)
BP-SCB-38	STRATEGIC PLANS & IMPLEMENTATION (BUPERS-02)
BP-SCB-11	TOTAL FORCE HUMAN RESOURCE OFFICE (BUPERS-05)
BP-SCB-42	INFORMATION MANAGEMENT OFFICE (BUPERS-07)
BP-SCB-46	BUSINESS TRANSFORMATION (BUPERS-08)
BP-SCB-47	PUBLIC AFFAIRS (BUPERS-332)
BP-SCB-17	RECORDS MANAGEMENT/DIRECTIVES (BUPERS-01)
BP-SCB-50	SAFETY OFFICE (BUPERS-00Z)
BP-SCB-51	SECURITY (BUPERS-00Y)

Illustration C - BUPERS High-Level (Organizational) Structure

Record Number /	Title
BP-CMD-2	NAVY PERSONNEL COMMAND (NPC)
BP-SCB-54	OPNAV N135C
BP-SCB-52	CUSTOMER RELATIONS MANAGEMENT (PERS-1)
BP-SCB-5	CAREER MANAGEMENT (PERS-4)
BP-SCB-3	CAREER PROGRESSION (PERS-8)
BP-SCB-2	RESERVE PERSONNEL MANAGEMENT (PERS-9)
BP-SCB-6	PERSONNEL INFORMATION MANAGEMENT (PERS-3)
BP-SCB-1	COMMAND ELEMENT (PERS-00)
BP-SCB-43	LEGISLATIVE/CONGRESSIONAL MATTERS (PERS-00L)
BP-SCB-37	BUSINESS OPERATIONS (PERS-5)
BP-SCB-53	IRREGULAR OPERATIONS/EMERGENCY MANAGEMENT

Illustration D - NAVPERSCOM High-Level (Organizational) Structure

(1) Container Naming Conventions. All containers (box and folder record types) as well as location types (organizations, positions and groups) will be prefaced with the

appropriate division or department (e.g., PERS-8, PERS-53, PERS-00J), followed by the name of the appropriate business function or process area.

Access Control:

a. Container Level

(1) Accessibility to the command, sub-command and unit boxes will be associated with the "BUPERS Organization," meaning that everyone at in the organization can see that these containers exist but, if they don't have access to view the folders inside, they will only see the box and nothing within.

(2) Only dataset administrators can make updates to the title and the security of these containers.

(3) Command or local administrators cannot create new containers at the box level, as it directly relates to the command organization structure.

b. Folder Level

(1) Yellow (section) folders are set to inherit permissions based on the "owner location" given to the folder when it is first created. For example, if you create a folder with NAVPERSCOM as the owner location, then all permissions within that folder to view, modify, update security settings, etc., will be open to everyone in NAVPERSCOM. In contrast, if a folder is created with the position of PERS-5B as the owner, then only that position will be able to view, edit, etc. the folders or documents contained within.

(2) All other folders (grey, teal and magenta) are set up to inherit the same security and access rights as the folder it is created under. For example, if a grey folder is created under a yellow folder whose security is such that all of NAVPERSCOM can view the contents of the folder but only PERS-5B can modify it or update its security settings, then the grey folder will inherit those exact permissions unless modified. The security settings on a folder can be modified at any time as long as you have permission to do so. Contact your local administrator if you think a folder's permissions are incorrect.

3.2. Standard Dataset Configuration Settings

3.2.1. Security Levels:

a. Unclassified is the only security level and For Official Use Only (FOUO) is the default security caveat.

b. TRIM locations are automatically assigned as "Unclassified, FOUO" via a predefined usage profile (i.e., profile power user group, local administrator group, etc.)

c. Folders and documents automatically inherit a security level of "Unclassified, FOUO."

d. Organizations, positions and group locations need to be assigned "Unclassified" security level since access is often give at the organization or position level.

3.2.2. Record Types. Utilization of standard set of record types is recommended. Creating a new record type must be warranted and approved by dataset DRM and dataset administrator.

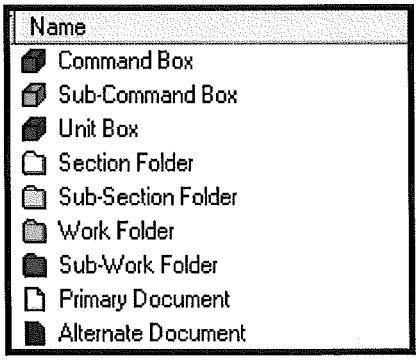

Illustration E - Command Default Record Types

3.2.3. Locations. No locations should be deleted from TRIM since they may have associated records or metadata. For instructions on what to do with employees leaving the command or transitioning to a new code (see Business Rule 4.2.2).

a. Creating an Organization, Group or Position. Groups must have at least the following fields and tabs populated:
General: Name of the location, beginning with the PERS-code

Associations: Add all organizations or groups to this location as required.

b. Profile. Security (Unclassified and FOUO), user category of "Information Worker".

4. BUSINESS RULES

4.1. Locations (Person, Positions, Organizations, Teams)

4.1.1. Business Rule - Each department or organization at a minimum must designate two command or local administrators. For larger organizations, additional local administrators may be designated as warranted. It is recommended that an organization maintain one administrator per every 50 personnel.

4.1.2. Business Rule - Command or local administrators must ensure user accounts and access rights are deactivated for all employees leaving or transferring from the command. To do this:

a. Uncheck the "Internal" box on the General tab so the user appears as external to the organization.

b. Deactivate the person's location on the Profile tab (uncheck "Accepting Network Logins" box).

d. Reassign the person to the external group titled "Deactivated BUPERS Users" on the Associations tab.

e. Optional - the date inactive field on the Active tab can be populated for record purposes.

4.2. Title and Naming Convention

4.2.1. Business Rule - The top three level containers should be named to identify the organization, command, department, or division.

4.2.2. Best Practice - Command names: Command short name is authorized.

4.2.3. Best Practice - The command RM and the BUPERS DRM will determine and create the first and second level record or container structure and naming convention.

4.2.4. Best Practice - departments, divisions, and work center Codes: department, division, and work center noun names and offices codes will be used e.g., PERS-532 Printing Service.

4.2.5. Best Practice - Container and folder names will start with a capitalized letter for each word used in the title. A record description in the **Notes** tab is recommended to be completed and describes the purpose and or type of information that will be contained in the record. Acronyms should be spelled out in the record **Notes** area.

4.2.6. Best Practice - When creating records, ensure that a location is first established and assigned to the owner location field in the properties prior to creating additional sub containers or folders. This will allow access rights to be inherited to the subfolders from the first container created. Otherwise, all subsequent records will need to have access rights added to each individual record.

4.3. Records and Document Storage

4.3.1. Business Rule - TRIM is the preferred means for document storage. Once documents are sent to TRIM, they must be deleted off of local share drives. The deletion records from individual desktops and or e-mail inboxes is a best practice. TRIM should be the primary copy of all official records.

4.3.2. Business Rule and Best Practice - When all the data in a share folder is moved into TRIM, a temporary reference link may be placed in that old share drive folder. This will point end users directly to the folder in TRIM where the documents are stored. This will facilitate a smooth transition to TRIM, and allow for quick and easy access to the data.

4.3.3. Business Rule - All calendar (CY) or fiscal (FY) folder must have the date created set to the 31 December of that CY year. This will allow proper disposition to trigger correctly via TRIM. All records will be granted proper disposition with some overlap i.e., records placed in CY-2010 folders in January will be granted proper disposition plus an additional 11 months of shelf life. Items placed in CY folders on 31 December will be granted exact day for day disposition without overlap. The disposition of the SSIC is triggered by the date created of the CY or FY folder.

4.3.4. Business Rule - dated closed shall be set to 31 December of that CY. This will prevent additional documents to be placed in previous year folders by end users. Common and or local administrators' profile will allow them to bypass the closure of folders.

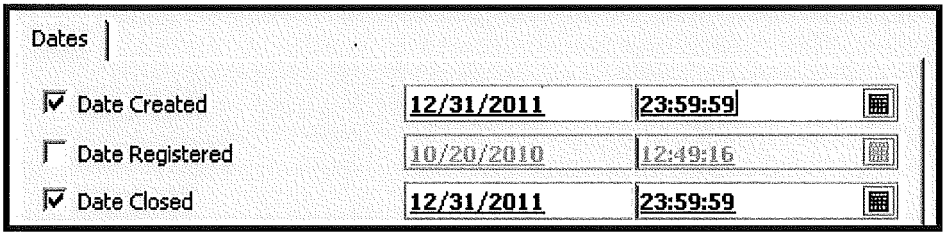

Illustration F - Setting date created and date closed

4.4. Security and Access

4.4.1 Business Rule - If folders are locked down to just one person or a small group of people, access must be granted at the POSITION level, not the individual.

4.5. Workflows

4.5.1. Business Rule - All workflow templates must be named with originator's office code along with meaningful title of process e.g., PERS-95 Line of Duty (LOD) or PERS-55 Weekly Report. This will make it easier to search for template by conducting a workflow name and title search.

4.5.2. Business Rule - All active workflows must be named with originator's office code along with meaning and distinctive title of process, e.g., PERS-95 Hobbs 1234(last four) LOD (abbreviated title). This will make it easier to search for active and or completed workflows by conducting a workflow name and title search.

4.6. Saved Searches

4.6.1. Business Rule - All saved searches shall be titled with organization code along with meaning and distinctive title of search, e.g., PERS-9X Monthly TRIM Records Count.

5. BEST PRACTICES

5.1. Locations (Person, Positions, Organizations, Teams)

5.1.1. Best Rule - An individual can belong to several locations or groups.

5.1.2. Best Practice - All section folders (yellow) must have the proper owner location assigned to them prior their creation.

This effects the default security settings on the subsequent folders or documents dropped into this folder.

5.1.3. Best Practice - Do not assign an individual location as an owner of a record(s). Instead, assign an organization or position to records containers, folders, and documents; then when an individual leaves, the ownership of the record does not have to change. All organizations and positions must start with the organizational code prefix, e.g., PERS-91B Branch Head or PERS-5 DIVDIR.

5.1.4. Best Practice - Check access or security on any type of record by right-clicking on the record, then selecting audit or security or have access control field as active field in view pane.

5.2. Title and Naming Convention Folders and Records

5.2.1. Best Practice - Container and folder names should be in title case. A record description in the notes tab that describes the purpose and or type of information that will be contained in the record is recommended.

5.2.2. Best Practice - Record or container properties will have the titling behavior option set to "Display Warning". This will cause a warning to be displayed when duplicate titles are being created in the dataset. Duplicate titles are authorized; however, consideration should be given to the reason the title is being duplicated and if there is an alternative title.

5.2.3. Best Practice - When creating records, ensure that a location is first established and assigned to the owner location field in the properties prior to creating additional sub-containers or folders. This will allow access rights to be inherited to the subfolders from the first container created. Otherwise, all subsequent records will need to have access rights added or changed in the future.

5.3. Records and Document Storage

5.3.1 Business Rule - Storing PST files in TRIM is not authorized. The TRIM document viewer will not open PST file formats. Only emails pertaining to official Navy business should be cataloged in TRIM, in the appropriate folder or

process area. E-mails should not be dumped into a general e-mail folder unless the e-mails truly do not correspond to a specific category or function.

5.3.2. Best Practice - Place duplicate and inadvertent records in command or organization trash can folder. Discarded records will be collected bi-weekly on the 2nd and 4th Friday of every month by command administrators. Records will be kept for 30 days and then deleted.

5.3.3 Best Practice - The default TRIM Setting in Outlook should be set to "**Primary Document**" record type. Using this default will eliminate the need for the user to select the record type each time an e-mail is cataloged. The user will need to change the record type to "**Alternate Document**" if they wish to file a document or e-mail WITHIN another document (as opposed to within a folder). **Alternate Documents** can include attachments, enclosures, history or background information, decisions, working papers, e-mail correspondence, etc.

APPENDIX A

TRIM QUICK REFERENCE GUIDES

Users are strongly encouraged to reference the robust TRIM online User Guide, which is available via "Start > Programs > TRIM Context > TRIM User Guide."

Where to Find More TRIM Help Documents and Quick Reference Guides:

TRIM Container Titled: "TRIM Help Documents/Quick Reference Guides" (Record Number BP-SEC-11-37)

LIST OF TRIM QUICK REFERENCE GUIDES

DoD Records Management and TRIM - Record Number BP-SEC-10-32

DoD Records Management Policy
What is TRIM Context?

Opening TRIM for the First Time - Record Number BP-SEC-11-37

Connect to the NAVPERSCOM server (region specific) and NAVPERSCOM dataset

Search for "NPC Dataset" and "TRIM End User Guides and Tutorials"

Save to Favorite "Records" & Setup "Favorite Records" to open at TRIM startup

TRIM Workflow Basics - Record Number BP-DOC-11-10776

Instructions for Initiating a Workflow BP-DOC-10-99995

E-mailing TRIM Documents - Record Number BP-DOC-09-14

Configuring e-mail profile in TRIM and sending e-mail from TRIM

Registering Documents (Queue Process) - Record Number BP-DOC-10-7976, PG 75-90

Adding multiple records to TRIM using the queue process

APPENDIX B

GLOSSARY OF TERMS

1. BUPERS Records Manager - person responsible all faucets of record management throughout BUPERS activities.

2. Dataset Records Manager - person responsible for the deployment and sets overall TRIM policy for TRIM throughout BUPERS activities.

3. Dataset Administrator - person(s) identified to serve as the command-wide TRIM administrator. This person also provides instructor-led training to end users and administrators as well as over-the-shoulder and ad-hoc support to BUPERS end users.

4. Documentary Materials. A collective term for Federal records, non-records materials, and personal papers that includes all media containing recorded information whatever the method or circumstance of recording. Federal records may be created on any physical media. The method of recording information may be manual, mechanical, photographic, electronic, or any combination of these or other technologies.

5. Command Records Manager - person responsible for records management throughout command.

6. Command or Local Administrator - person(s) identified to serve as a TRIM administrator for the respective code, department, or division.

7. National Archives and Records Administration (NARA) - The organization and agency responsible for appraising, accessioning, preserving, and making available permanent records. NARA is responsible for implementing records management laws within the Federal Government.

8. Non-Record Materials - Information and documents not meeting the definition of a "Federal record." These materials may be destroyed when no longer needed. This includes Federally owned materials that are:

a. Not created or received under Federal law or in connection with government business;

b. Not preserved or considered appropriate for preservation because they lack evidence of agency or component activities or information of value; or

c. Extra copies of documents kept only for convenience or reference.

9. Permanent Records - Any record with enduring value of a historical, research, legal, scientific, or cultural nature, and that documents primary missions, functions, responsibilities, or significant experiences and accomplishments.

10. Personal Records or Papers - Materials belonging to an individual that are not used to conduct agency business. They are related solely to an individual's own affairs or are used exclusively for that individual's convenience. Correspondence designated "personal" or "private," but relevant to the conduct of public business, is an official record and must be managed per this instruction.

11. Record - The term "record" includes all books, papers, maps, photographs, machine-readable materials, or other documentary materials, regardless of physical form or characteristic, made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value of data in them. In short, a "record" is any document or material made or received in the course of government business, which is or should be kept either as evidence of the conduct of business or because it contains valuable information. The electronic format has no bearing on whether the information is a record.

12. Records Management - The planning, controlling, directing, organizing, training, promoting, and managing activities involving information requirements, records creation, records maintenance and use, records preservation, and records disposition of all Federal agency records.

13. Standard Subject Identification Code (SSIC) - A method for categorizing and subject classifying Navy and Marine Corps

information that ensures documents are filed consistently and can be retrieved quickly. A SSIC is a four or five-digit number that categorizes the subject of a document. A SSIC is required on all records including, but not limited to, letters, messages, directives, forms, and reports. The SSIC is to be used in conjunction with reference (c), which describes specific records and provides disposition schedules for them.

14. Temporary Record - Any record that does not qualify as a permanent record. Most Naval Criminal Investigative Service files fall under this category. Examples include leave applications, equal employment opportunity program files, personnel files, general correspondence, security logs, etc.

15. Vital Records - Records essential to the continued functioning or reconstitution of an organization during and after an emergency and also those records essential to protecting the rights and interests of the organization and of the individuals directly affected by its activities. Vital records include both emergency operating and rights-and-interest records. These records are considered part of an agency's continuity of operations plan.