



DEPARTMENT OF THE NAVY
COMMANDER, NAVY INSTALLATIONS COMMAND
2713 MITSCHER ROAD, SW
ANACOSTIA ANNEX, DC 20373-5802

CNICINST 5210.1
N00

MAY 22 2008

CNIC INSTRUCTION 5210.1

From: Commander, Navy Installations Command

Subj: COMMANDER, NAVY INSTALLATIONS COMMAND RECORDS
MANAGEMENT PROGRAM

Ref: (a) SECNAVINST 5210.8D
(b) SECNAV M-5210.1
(c) SECNAV M-5210.2
(d) SECNAVINST 5216.5D
(e) Title 44 U.S.C. Chapters 29, 31, and 33 (Records Management and Disposal of Records)
(f) Title 36 U.S.C. Chapter 12, Part 1234 (Electronic Records Management)
(g) DOD Directive 5015.2-STD, Design Criteria Standard for Electronic Records Management Software Application, 25 Apr 07
(h) SECNAVINST 5510.36
(i) SECNAVINST 5720.42F

Encl: (1) Glossary
(2) Sample File Plan
(3) Additional Duty Appointment Format
(4) TRIM Best Practice Guide
(5) Records Management Self Assessment Checklist

1. Purpose. To issue Commander, Navy Installations Command (CNIC) Records Management Program policies to ensure administrative information created or acquired by activities and offices is properly managed from creation/receipt through final disposition according to Federal laws and Department of the Navy (DON) Records Management Program requirements per references (a) through (i).

2. Policy. CNIC activities will establish, maintain, and dispose of records consistent with the guidance in references (a) through (i).

MAY 22 2008

3. Applicability and Scope. This instruction applies to all military, civilian, and contractor personnel assigned to activities within the CNIC domain.

4. Definitions. Special terms used in this instruction are explained in enclosure (1).

5. Records Management. Commands are required by law to maintain an active records management program that provides for the accurate and efficient tracking and retrieval of command records. Command records must adequately document the organization, operations, functions, policies, procedures, decisions, and transactions of the command and provide information necessary to protect the legal and financial rights of the command and the government. The CNIC Records Management Program is designed to ensure records are maintained and disposed of per references (a) through (i).

6. Records Creation

a. All personnel are responsible for creating, maintaining, and preserving information as records, from any type of media, sufficient to provide evidence of organization, functions, policies, procedures, or decisions; or records that document the transactions necessary to protect legal and financial rights of the command and its personnel.

b. Records will be properly identified by their Standard Subject Identification Code (SSIC). SSICs are critical in determining disposition authority and, per reference (c), shall be used on all official records created, including electronic mail (e-mail), letters, memorandums, messages, directives, forms, and reports.

c. In order to minimize the recordkeeping burden of e-mail recipients and to avoid unnecessary burden on the electronic communications system, both the creator and recipient of an e-mail message must decide whether it is a record. Therefore, a document may be a record in more than one office or activity.

7. Records Retention and Disposal. Records management is not complete without a system in place for the proper retention and disposal of records. The disposition guidance contained in reference (b) is mandatory and will be followed. Requests for exceptions to disposal guidance must be forwarded to the CNIC Records Manager for appropriate review and approval by the DON

MAY 22 2008

Records Manager (CNO (DNS 5)). Disposition is divided into two categories:

a. Permanent Records. All records identified in reference (b) as permanent must be transferred to the National Archives and Records Administration (NARA) when no longer needed for administrative, legal, or fiscal purposes. The specific retention period before transfer is normally specified in the record's disposition. NARA can accept permanent records in paper or electronic media that meets the provisions of reference (b) or standards applicable at the time of the transfer.

b. Temporary Records. Temporary records must be retained for the period specified in reference (b) and then destroyed or deleted. Federal Records Centers (FRC) can store temporary records with retention periods of three years or longer.

8. Records Freezes and Holds. Regardless of the retention standards established by reference (b), records pertaining to unsettled claims for or against the Federal Government, current or pending litigation, preservation orders, Freedom of Information and/or Privacy Act requests, exceptions taken by the General Accounting Office or internal auditors, or incomplete investigations will not be destroyed. The records must be retained until the litigation or action is settled, the investigation is completed, the preservation order is lifted, or the exception is cleared. Records identified as frozen or held may not be destroyed without written notification of their release from the Command Records Manager and/or Command SJA/Counsel. Segregate and retain records directly pertinent to the litigation, investigation, preservation orders, or exception until all actions are completed. Before implementing such procedures, coordinate with the Command Records Manager and the Command SJA/Counsel to establish the legitimacy of the action and your proposed implementing actions.

9. 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. Reference (b), Part I, paragraph 17, and reference (d), Chapter 1, Sections C and D, provide general recordkeeping procedures for electronic records

MAY 22 2008

and e-mail and are supplemented by the specific guidance contained in this instruction. 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" contained in the Federal Records Act (reference (e)).

10. Records Filing. Filing procedures constitute an integral part of any records management program. Reference (c), Chapter 1, provides guidance for establishing filing procedures for records created and maintained in offices and activities. Use of these procedures establishes a systematic way that is consistent throughout the command and meets the procedural requirements of references (c) and (d). Procedures in reference (c), along with amplifying guidance in this instruction, are to be used by personnel responsible for maintaining command records.

a. Filing Procedures for Hardcopy Records. Command files will be centralized and maintained by the Command Records Manager, but they may be decentralized and maintained by individual departments. The decision to have centralized or decentralized files depends on the mission of the activity and a determination by the activity head as to which method is most efficient for the accomplishment of the activity's mission. Whether activities are using centralized or decentralized files, a file plan is required for their files. Enclosure (2) is a sample file plan and is to be used as a guide to create all file plans.

b. Filing Procedures for Electronic Records. The DON mandated Electronic Records Management (ERM) solution is Tower Software's Total Records and Information Management (TRIM) Context, which has been provided via 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 per references (a) through (g) for filing electronic records. Activities with access to the NMCI network will use the TRIM Context program. TRIM is the DON standard and is approved and authorized in accordance with reference (g) for storage of electronic records including e-mail. The CNIC TRIM dataset has been deployed at the echelon 2 level and is being implemented throughout the rest of the CNIC Echelon III/IV Commands. Once TRIM is deployed at a

MAY 22 2008

command, its use is required to properly categorize records by records series (SSIC) and to file and manage them until final disposition is mandatory. A file plan is required for records stored in TRIM. Enclosure (2) is a sample file plan and is to be used as a guide to create all file plans. Electronic records stored in other Navy enterprise-wide programs, i.e., EMPRS, are exempt from the requirement to use TRIM.

(2) Until TRIM is fully deployed and operational within CNIC commands, 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 their final disposition per reference (b), Part III, and this instruction. In all cases the permanent deletion of electronic records when not printed and filed must meet the disposition guidance contained in reference (b), 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 (g). 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 CNIC Records Manager for review and approval by CNIC Chief Information Officer (CIO).

11. Facsimile (Fax) Transmission Records. Section E of reference (d) provides information on the use of facsimiles and their use as official records. As with other records, the retention, filing, and disposal of official government facsimile records must conform to the guidance contained in reference (b) and this instruction.

12. Personal Data. All persons having records containing Personally Identifiable Information (PII) data must exercise reasonable caution to ensure that this information is protected. PII is defined as any information about an individual maintained by an agency including, but not limited to, education, financial transactions, medical history, and criminal or employment history, and information which can be used to distinguish or trace an individual's identity, such as their name, SSN, date and place of birth, mother's maiden name, biometric records, and any other personal information which is linked or linkable to an individual. PII is subject to protection and must be marked "FOR OFFICIAL USE ONLY - Privacy Sensitive: Any misuse or unauthorized disclosure may result in both civil and criminal penalties." Reference (i) contains additional information concerning protection and destruction of PII.

MAY 22 2008

13. E-Mail Records. Within CNIC, e-mail is authorized to convey official correspondence, to include information meeting the definition of a "Federal record," and informal information subject to the limitations discussed in reference (d). E-mail users are:

a. Required to preserve e-mail messages and any attachments that document CNIC organization, functions, policies, decisions, procedures, and operations meeting the standards as a Federal record. They may be retained in an electronic format or printed out for filing. Regardless of medium, file and dispose of them as required per references (b) and (c) and this instruction.

b. Required to file e-mail messages (with the transmission data and, when determined necessary to document the actual receipt by addressee(s), receipt data) and attachments determined to qualify as Federal records. If printed out and not saved electronically, they must be filed in the activity hardcopy filing system so that they can be found when needed by those persons authorized to access the activity's records.

c. Authorized to use the e-mail system to transmit as an attachment formal correspondence within the Department of Defense (DoD). When using e-mail in place of formal correspondence, the drafter must follow the procedures outlined in reference (d). When using e-mail for this purpose, use standard correspondence formats including SSIC, serial number, date, and signature authority. In place of the signature, type in your letterhead information and use "/s/". Transmit only from your authorized e-mail address and retain a copy of the e-mail transmittal and attached correspondence as your activity's record copy. Refer to reference (d) for additional information on electronic and e-mail records.

14. Personal Records or Papers. When retaining records that are personal and not Federal records, they must be clearly marked "Personal Papers" and kept separate from the activity's official records. Additional guidance is contained in reference (b), Part I, paragraph 14.

15. Removal of Files Upon Transfer or Retirement. Individuals who are transferring or retiring may not remove official records from their offices. They may remove personal files at their discretion without agency permission. Extra copies of official records may be removed upon approval by the activity's Records Manager. Approval may be granted only if all of the following conditions are met:

MAY 22 2008

- a. Removal will not diminish official records.
- b. Removal will not exceed normal administrative economies.
- c. The materials do not contain national security classified information. (An exception may be granted when moving to another activity that is authorized to store classified defense information.)
- d. The information removed is not subject to the Privacy Act of 1974, as amended.
- e. Disclosure of the information removed is not otherwise prohibited by law.

16. Vital Records. Each activity must incorporate a Vital Records Program per reference (b), Appendix H. Each activity must develop a file plan (enclosure (2)) that identifies records necessary for the activity to accomplish mission essential functions without unacceptable interruption during a national security emergency, or other emergency or disaster, and also protects the legal and financial rights of CNIC employees and individuals directly affected by its activities. Electronic filing in TRIM is the recommended method of maintaining Vital Records.

17. Responsibilities

a. CNIC Command Administration Program Manager

(1) As the designated CNIC Records Manager, implement and monitor the DON Records Management Program within CNIC.

(2) Appoint a Dataset Records Manager (DRM) who will maintain final authority over the CNIC TRIM dataset for electronic management of records.

b. CNIC Staff Judge Advocate/Office of General Counsel. The CNIC Staff Judge Advocate/CNIC Office of General Counsel will support the CNIC Records Management Program by providing legal assistance to CNIC 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 CNIC managed records.

c. CNIC Command Information Officer (CIO)

MAY 22 2008

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

(2) Ensure that application developers and system administrators include records management plans and procedures that comply with NARA in all configuration management. Electronic records should be migrated in full to a new system or converted to an appropriate software or hardware format when their current electronic information system is assessed for termination.

(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) Provide technical assistance to the CNIC Records Manager/DRM to ensure CNIC complies with the electronic Freedom of Information Act requirements and Privacy Act requirements.

d. CNIC Security Manager. The CNIC Security Manager will provide technical support for issues pertaining to the proper classification and management of classified records.

e. CNIC Records Manager

(1) Exercise primary oversight responsibility for the CNIC Records Management Program.

(2) Act as liaison with the DON Director of Records and CNIC activities' Records Managers.

(3) Conduct or oversee inventory of all organization records and ensure compliance with organizational and Navy directives for storage.

(4) Review and forward requests to store electronic records in any system other than TRIM or other Navy enterprise-wide program to CNIC Deputy CIO.

(5) Review and update this instruction, as required, at least annually.

(6) Ensure Command Records Managers are trained annually in areas such as the creation, maintenance, use, and disposal of files; file plans; storage/archiving policies and procedures;

MAY 22 2008

and TRIM. Enclosures (1) through (5) are provided as training and guidance.

f. CNIC Dataset Records Manager

(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 CNIC TRIM dataset.

(4) Monitor and troubleshoot CNIC's TRIM dataset.

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

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

(7) Provide training to Command Local TRIM Administrators.

g. Commands

(1) Implement the DON Records Management Program at Region and Installation level per references (a) through (i) and this instruction.

(2) Appoint in writing a Command Records Manager to ensure records are maintained per this and other relevant instructions, regulations, and laws. Enclosure (3) is a sample Records Manager appointment letter.

(3) Provide copies of the Command Records Manager's appointment letter and contact information, and any subsequent changes, to the next higher echelon Records Manager/Officer.

h. Command Records Manager

(1) Maintain a listing of, and act as a liaison with, Records Managers at the next higher and lower levels.

(2) Ensure Records Management Program implementation at all levels within their activity and provide appropriate level

MAY 22 2008

of guidance to ensure effective continuity of the command's Records Management Program.

(3) Ensure command compliance with records management policies and guidelines as set forth in references (a) through (i) and this instruction. This includes, but is not limited to:

(a) Using enclosure (2) to institute and maintain a command file plan.

(b) Conducting or overseeing an annual inventory of all activity records.

(c) Completing an annual review and inspection of local disposal procedures for the activity's records to ensure records disposal and retention procedures are current, adequate, and applied per reference (b).

(d) Notifying the CNIC Records Manager when unscheduled records are located and ensuring that they are not destroyed pending receipt of proper authority from NARA.

(e) Originating or approving all requests to dispose or transfer records.

(f) Maintaining the command's Vital Records Program and reviewing procedures annually.

i. Command Local TRIM Administrators. Local TRIM 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 CNIC DRM. Local Administrators will:

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

(2) Serve as first line of support to end users within the command/departments.

(3) Assure all TRIM folders and documents in their area of responsibility have the proper retention (SSIC) and security applied to them.

(4) Create workflows for sections as needed.

MAY 22 2008

(5) Provide access to TRIM for new employees.

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

(7) See enclosure (4) 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.

18. Training. Command Records Managers and local TRIM Administrators are required to complete the four courses listed in subparagraph 18a below and make a recommendation to the local chain of command as to who in the command should take these courses.

a. These electronic training courses are available on Navy E-learning available through Navy Knowledge Online (NKO).

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

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

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

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

b. Records management procedures and guidance are available in the following references:

(1) Records Management and Procedures for Disposition: Reference (b), Part I;

(2) Applying Records Retention Standards: Reference (b), Part II;

(3) Federal Records Center Transfer Procedures: Reference (b), Appendix A;

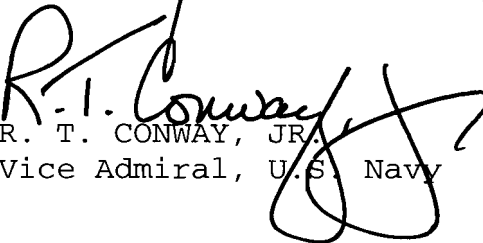
(4) Vital Records Program: Reference (b), Appendix H;

(5) Filing Procedures: Reference (c), Chapter 1;

MAY 22 2008

c. TRIM Help Documents. In addition to the training and guidance in enclosure (5), there are several TRIM help documents in the CNIC TRIM dataset. These documents are in the box labeled TRIM Help Documents, which is the CNIC Headquarters (HQ) command box. A title word search in TRIM for the word "TRIM" or "help" will also display the CNIC HQ Command Box.

19. Point of Contact. The point of contact for the CNIC Records Management Program shall be the CNIC Records Manager.


R. T. CONWAY, JR.
Vice Admiral, U.S. Navy

Distribution:

Electronic only, via CNIC Portal

<https://cnicportal.cnic.navy.mil/HQ/N00/Directives/Forms/AllItems.aspx>

MAY 22 2008

GLOSSARY

1. 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.
2. National Archives and Records Administration (NARA). The organization/agency responsible for appraising, accessioning, preserving, and making available permanent records. NARA is responsible for implementing records management laws within the Federal Government.
3. 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.
 - c. Extra copies of documents kept only for convenience or reference.
4. 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.
5. 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 in accordance with this instruction.
6. Record. Per reference (f), the term "record" includes all books, papers, maps, photographs, machine-readable materials, or other documentary materials, regardless of physical form or

MAY 22 2008

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.

7. 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.

8. 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. Per references (c) and (d), an 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 (b), which describes specific records and provides disposition schedules for them.

9. Temporary Record. Any record that does not qualify as a permanent record. Most NCIS files fall under this category. Examples include leave applications, Equal Employment Opportunity Program files, personnel files, general correspondence, security logs, etc.

10. 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 (COOP).

| CNIC SAMPLE FILE PLAN BY STANDARD SUBJECT IDENTIFICATION CODE (SSIC) (REVISED 05/20/08) | | | | | |
|---|--|---|--------------|-------------------------|-----------------------------|
| FILE NUMBER | FILE TITLE | DISPOSITION INSTRUCTIONS | VITAL RECORD | IDENTIFICATION OF MEDIA | LOCATION |
| 4220.1b(1) | General Contracting Records 1. Contracting Records b. Routine Procurement Files (1)(a) Transactions of more than \$25,000 | Destroy 6 years and 3 months after payment. | No | Electronic | TRIM |
| 4220.1b(2) | General Contracting Records 1. Contracting Records b. Routine Procurement Files (1)(b) Transactions of \$25,000 or less | Destroy 3 years after final payment. (Close file at end of FY, retain 3 years, and destroy, except those files on which actions are pending shall be brought forward to the next FY's files for destruction therewith.) | No | Paper & Electronic | Central Office Files & TRIM |
| 4570.2 | Excess & Surplus Property Records 2. Report of excess & surplus property | Destroy 1 year after final action has been taken. | No | Paper | N8 Department Files |
| 5000.2 | General Administration & Management Records 2. Activity's administration operation | Destroy when 2 years old. | No | Electronic | TRIM |
| 5000.11a | General Administration & Management Records 11. Additional Duty Designation Records a. When filed separately | Destroy on expiration, revocation, or suppression of designation. | No | Paper & Electronic | Central Office Files & TRIM |
| 5000.12a | General Administration & Management Records 12. Administrative Agreement Records a. Understandings or agreements not involving transfer of personnel billets and material | Destroy 3 years after suppression, cancellation, or termination of the agreement. | Yes | Paper & Electronic | Central Office Files & TRIM |
| 5040.3e(2) | Naval Command Inspection Program Records 3. Survey & inspection report files e. Other activity report files (2) All other activities report files | Destroy when superseded. | No | Electronic | TRIM |

| FILE NUMBER | FILE TITLE | DISPOSITION INSTRUCTIONS | VITAL RECORD | IDENTIFICATION OF MEDIA | LOCATION |
|-------------|---|---|--------------|-------------------------|-----------------------------|
| 5050.1c | Meetings, Conferences, Conventions, & Visits Records 1. Minutes & reports, of meetings, conferences, conventions, & visits c. All other copies | Destroy when purpose is served. | No | Electronic | TRIM |
| 5220.1 | Workload/Performance Measurement Records 1. Work measurement files | Destroy when 1 year old. | No | Paper | Central Office Files |
| 7300.1 | General Appropriation, Fund, Cost, and Property Accounting Records 1. General Correspondence Files | Destroy when 3 years old. | Yes | Paper | Central Office Files |
| 7302.1b | Fund Accounting Records 1. Obligation Documents b. All other copies | Destroy when 2 years old or 1 year after submission of final report of funds concerned, whichever is later. | Yes | Paper | Central Office Files |
| 7302.2a | Fund Accounting Records 2. Account ledgers, journals & records a. Subsidiary ledgers, journals & records | Destroy when 2 years old or 1 year after final report, whichever is later. | Yes | Paper | Central Office Files |
| 12610.2 | Hours of Duty Records 2. Time & attendance input records | Destroy when GAO audit or when 6 years old, whichever is sooner. | No | Electronic | SLDCADA & TRIM |
| 12610.3 | Hours of Duty Records 3. Overtime Authorization requests | Destroy when 4 years old. | No | Electronic | SLDCADA & TRIM |
| 12620.1 | Alternate Work Schedule Records 1. Documents showing alternative work schedules such as flextime & compressed schedules | Destroy when 2 years old. | No | Paper & Electronic | Central Office Files & TRIM |
| 12990.2a(1) | General & Miscellaneous Records 2. Duplicate documentation & personnel files maintained outside personnel offices a. Supervisor's personnel files (1) Annual review | Destroy when superseded or obsolete. | No | Paper | Central Office Files |

MAY 22 2008

Letterhead

5210
(Date)

From: Commanding Officer
To: Name of designated person

Subj: ADDITIONAL DUTY APPOINTMENT

Ref: (a) SECNAVINST 5210.8D
(b) SECNAV M-5210.1
(c) SECNAV M-5210.2

1. Per reference (a), you are hereby appointed as the (name of command) Records Manager. As the Records Manager, you will become familiar with the contents of references (b) and (c) and other pertinent records management instructions.

2. As the (name of command) Records Manager, your duties are, but are not limited to, the following:

a. Overall administration of the command's Records Management Program to include the planning, controlling, directing, organizing, training, promoting, and other managerial activities involving records creation, records maintenance and use, records preservation, and records disposition.

b. Maintaining references on various aspects of the program for the purpose of reporting to higher authority.

c. Providing technical assistance to requesting offices.

d. Performing such management studies as are necessary.

e. Coordinating any general reviews of specific aspects of Records Management.

3. This appointment will not expire until canceled by me and may not be further delegated without my express permission.

COMMANDING OFFICER SIGNATURE

Copy to:
(Next higher command in echelon) Records Manager

Enclosure (3)

MAY 22 2008

BEST PRACTICE GUIDE
TO SUPPORT
TOTAL RECORDS INFORMATION MANAGEMENT (TRIM)
FOR THE
COMMANDER, NAVY INSTALLATIONS COMMAND
(CNIC)

MAY 22 2008

TABLE OF CONTENTS

SECTION 1 - INTRODUCTION

| | | |
|-----|---|---|
| 1-1 | Purpose | 1 |
| 1-2 | Background | 1 |
| 1-3 | Overview | 1 |
| 1-4 | Audience | 2 |
| 1-5 | Command/Department TRIM Local Administrator Responsibilities | 2 |
| 1-6 | Document/Records Storage | 2 |

SECTION 2 - GETTING STARTED WITH TRIM

| | | |
|-----|---|----|
| 2-1 | Personnel Assignment | 3 |
| 2-2 | Opening CNIC TRIM Dataset | 4 |
| 2-3 | Locations | 7 |
| 2-4 | Security | 11 |
| 2-5 | Record Types - Containers/Folders/Documents | 11 |
| 2-6 | Deleting Records/Documents | 15 |
| 2-7 | File Plan Attachment | 15 |
| 2-8 | Outlook Integration | 16 |

SECTION 3 - MISCELLANEOUS

| | | |
|-----|--|----|
| 3-1 | Search of Entire Dataset | 18 |
| 3-2 | Edit Documents | 18 |
| 3-3 | Toolbars | 18 |
| 3-4 | Removing Users With Records Checked Out | 19 |
| 3-5 | Reassigning Owner Locations | 20 |
| 3-6 | Dropped Files - Moving Multiple Documents Into TRIM | 22 |
| 3-7 | User Login Type Permission Table | 23 |

MAY 22 2008SECTION 1 - INTRODUCTION1-1. Purpose

a. The objective of this Best Practice Guide is to assist Command Records Managers and Local TRIM Administrators to get started and standardize the implementation of TRIM Context software across the CNIC enterprise. The goal is to efficiently and effectively manage, store, retrieve, and archive records within the CNIC TRIM dataset and to ensure that the CNIC content owners and records managers maintain records in a secure environment and perform consistent document management practices across the enterprise.

b. This guide is not designed as a stand-alone user manual for TRIM. This Best Practice Guide provides business rules and specific procedures for using TRIM in the CNIC dataset. To supplement the Best Practice Guide there are several TRIM training documents and user manuals available and recommended for use:

- Training documents, manuals, and PowerPoint presentations are available in the CNIC TRIM dataset, and can be found using the Title Word search "Help".
- TRIM electronic training courses are available on NKO.
- TRIM online User Guide is available by accessing **Start > Programs > TRIM Context > TRIM User Guide**.

1-2. Background. DOD Directive 5015.2 directs commands and personnel to manage official records efficiently and effectively as required by law. Per OPNAVNOTE 5210 of 28 July 2006, personnel retaining records must use the NMCI-provided DON Electronic Records Management (ERM) tool. Available on all NMCI seats, TRIM Context is the core application for both electronic and non-electronic storage and management of official DON records.

1-3. Overview. The DON ERM solution is Tower Software's TRIM Context, which was provided as part of the NMCI initiative. The TRIM software and server platforms are provided for under NMCI; however, the contents and management of those contents is the responsibility of the individual content owners. The goal of this guide is to ensure that CNIC content owners and records managers maintain records/documents in a secure environment and perform consistent document management practices across the enterprise.

MAY 22 2008

1-4. Audience. This document is intended for local command and/or department TRIM Administrators and Records Managers.

1-5. Command/Department TRIM Local Administrator Responsibilities

a. Before a command can access the CNIC TRIM dataset, the local command administrator must contact the CNIC Dataset Records Manager (DRM) to establish their high level command structure in TRIM and have access granted to the local administrators.

b. The local command and department administrator will also ensure each end user:

- Selects the CNIC dataset on log in
- Profile is correctly configured
- Assigned to a location/group
- Default access rights are correct
- Outlook is correctly configured
- Favorites are established for records (by record number, location, etc.)

c. Additionally, local command administrators will:

- Maintain a log of users that have been assigned as Local Administrators.
- Create workflow templates.
- Test the access rights assigned to records/containers to ensure that the proper controls have been implemented correctly.
- Ensure access rights are deleted for all employees leaving or transferring from the command (delete the member's location).

1-6. Document/Records Storage - Records to be Retained in TRIM

a. The initial set of records/documents being retained in TRIM are records/documents that are currently retained as command files/records in either paper or electronic format. Paper copies of files can be scanned and entered in TRIM as a PDF file based on command policy.

b. Additionally, the following documents should be retained in TRIM:

MAY 22 2008

- Any policy or decision paper signed by CNIC or a commanding officer or officer in charge
- Any official naval message released that provides policy or guidance
- Command directives
- Official letters signed by CNIC or a commanding officer or officer in charge
- Official press releases
- Memorandums of Understanding and Memorandums of Agreement between CNIC commands and outside commands
- Any document that provides a historical record of the organization, functions, policies, procedures, operations, decisions, and other activities of the organization
- Any other documents designated in accordance with applicable mandates
- Emergency operating records essential to the continued functioning or reconstitution of an organization after an emergency

c. The term "records" are documentary materials, in any medium to include e-mail, that satisfy the definition of a Federal record.

SECTION 2 - GETTING STARTED WITH TRIM

2-1. Personnel Assignment. In order to successfully implement TRIM, a staffing plan should be developed denoting the skill levels required to perform the task required by the role assigned in the TRIM application. The following provides guidelines in selecting personnel for the various TRIM roles. At a minimum, each command is required to have a command level local administrator and, depending on command policy and structure, local administrators may be assigned at the department level.

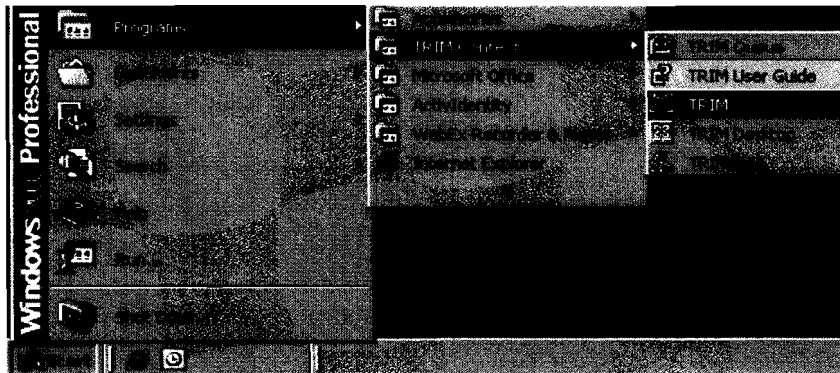
| Role | Skills | Business Knowledge |
|---------------------|---|---|
| Local Administrator | Mid level computer experience with detailed knowledge in assignment of security rights, application configuration, business process flows, file types, and networks | 1. Broad knowledge of the command's business functions 2. Understanding of the records management policies and governing regulations |

MAY 22 2008

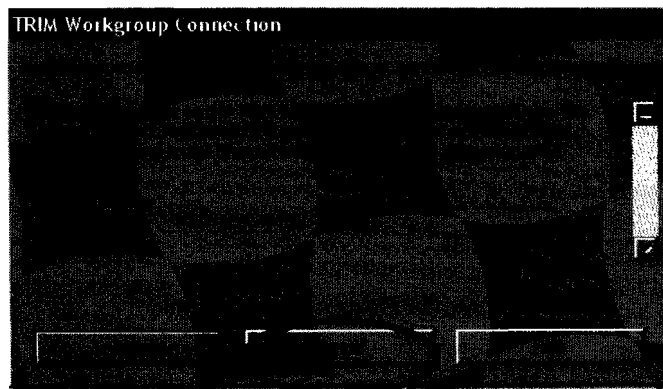
| | | |
|-------------------|--------------------|--|
| Power User | Advanced PC skills | Specific and in-depth knowledge of the business tasks, policies, and relationship to other business areas and their interface requirements |
| Advanced End User | Basic PC skills | Knowledge of records maintenance and filing |

2-2. Opening CNIC TRIM Dataset. Users must have an NMCI account (e.g., @navy.mil or @usmc.mil), and be logged in via their NMCI computer to access TRIM Context. On opening TRIM initially, the user is required to add a command dataset(s) to the Dataset Name list. By default, a dataset is not specified and must be added for the user to access the appropriate TRIM dataset. If done correctly these steps are only required the first time TRIM is launched.

- Click **Start** > **Programs** > **TRIM Context** > **TRIM** to open TRIM Context.

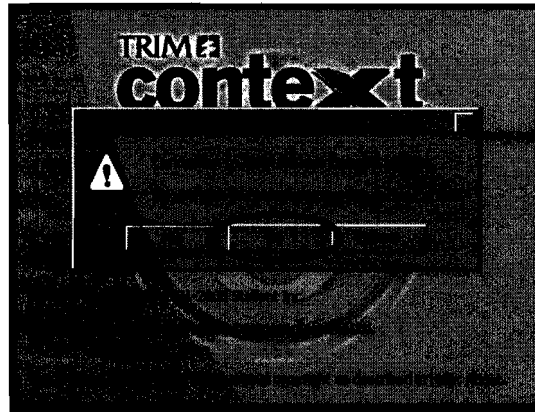


- The TRIM Workgroup Connection window will appear if TRIM could not connect to the specified TRIM Workgroup Server. Click **Cancel**.

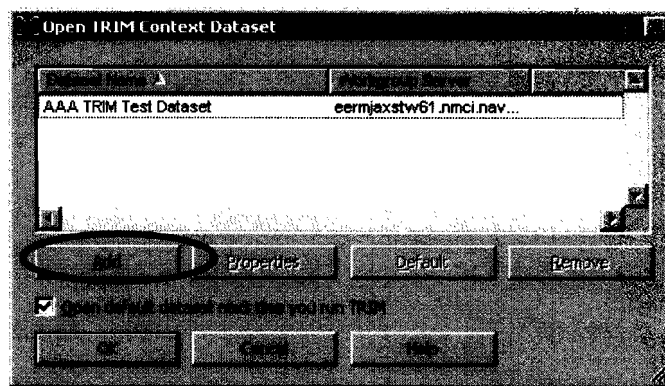


MAY 22 2008

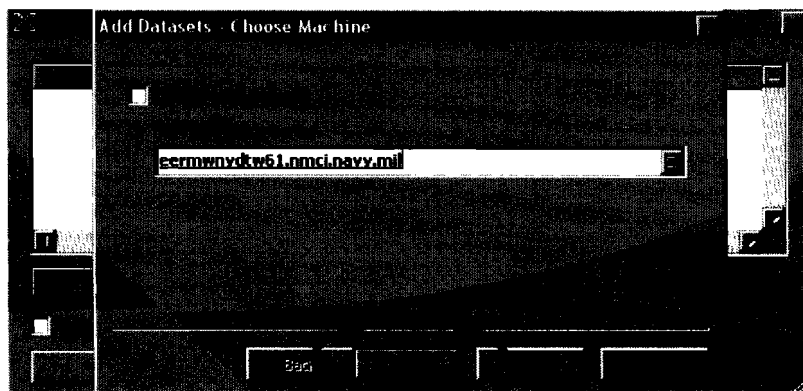
- Click **No** to continue to use the dataset offline.



- The Open TRIM Context dataset window will appear. Click **Add**.



- A second dialog box titled Add Datasets - Choose Machines will appear.



- Depending on the geographic location of the user, the appropriate TRIM Workgroup Server name should appear in the

MAY 22 2008

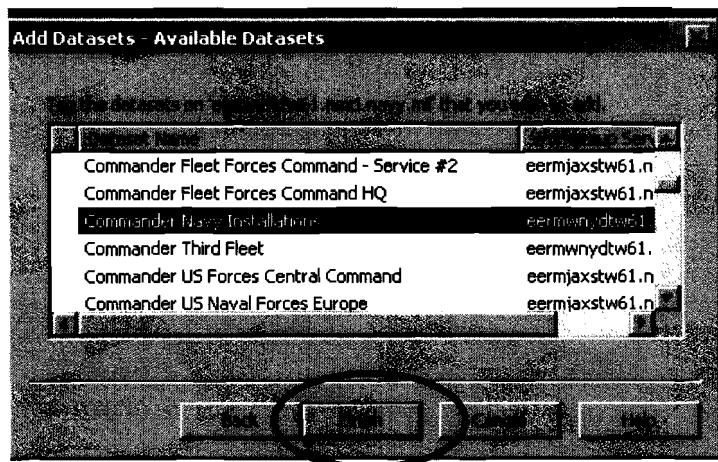
"Or TRIM Workgroup Server" field. Users should connect to one of the four geographic Primary TRIM Workgroup Servers:

- o Washington DC - eermwnydtw61.nmci.navy.mil
- o Norfolk - eermnrftw61.nmci.navy.mil
- o Jacksonville - eermjaxstw61.nmci.navy.mil
- o San Diego - eermsdntw61.nmci.navy.mil

- Backup TRIM Workgroup Servers are also accessible:

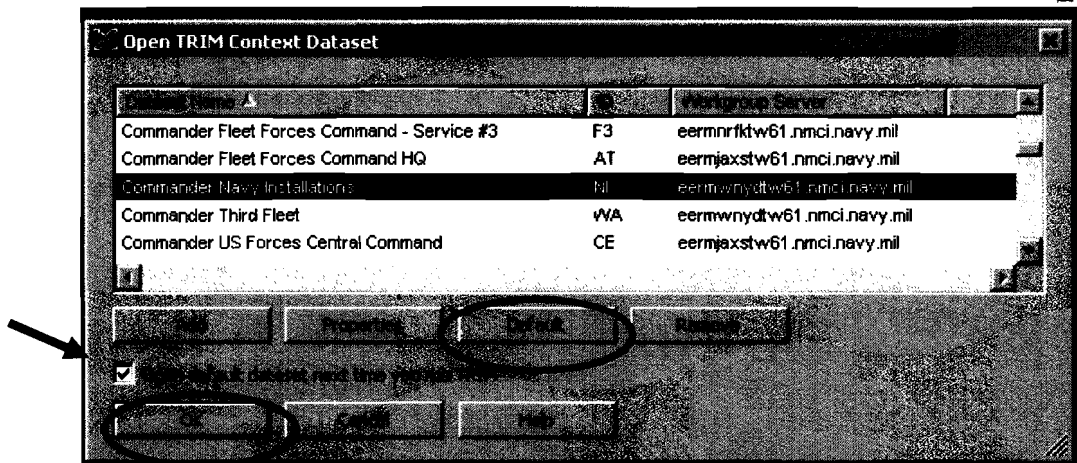
- o Washington DC - eermwnydtw62.nmci.navy.mil
- o Norfolk - eermnrftw62.nmci.navy.mil
- o Jacksonville - eermjaxstw62.nmci.navy.mil
- o San Diego - eermsdntw62.nmci.navy.mil

- Note - Do not select the Choose Local Datasets option.
- Click **Next**.
- The available TRIM datasets will be listed. Select (tag) the CNIC TRIM dataset (CNIC dataset is called **Commander, Navy Installations Command**.) Click **Finish**.



- The **Open TRIM Context Dataset** window will show the selected TRIM datasets. Highlight **Commander, Navy Installations Command**, click on the **Default** button, place a check mark in the **Open default dataset next time you run TRIM**, and click **OK** to enter the TRIM dataset.

MAY 22 2008



NOTE: If a user has not been added to the CNIC TRIM dataset, or if the user location is not correct, the user will not be able to access the CNIC TRIM dataset.

2-3. Locations. Location is a broad term that refers to the users and groups in TRIM. Locations can be the command, department, division, workgroup, etc., or individuals. The security and access rights for the location must match the security and access rights of a record in order for individuals in a location to view the record.

Best Practice - Assign every individual in the CNIC dataset to an organizational location and/or working group location.

2-31. Creating a Location

a. To create an organization or group:

- Select **Tools > Locations > All** from the menu bar to bring up all the locations.
- To find the correct parent organization, begin typing the name and press **Enter**.
- Right click on the organization and select **New Child Location > New Child Organization**.
- For all locations except **Person** at a minimum complete:
 - o General Tab
 - Enter the name of the location (see **2.41 Title/Naming Convention** below for correct format).
 - Select the **Internal** radio button with a check mark.
 - o Profile Tab
 - Place a check mark in the **Use Profile of** and then select the group profile (normally the **Advanced Enduser Group** - see below **2.32 User Type**).

MAY 22 2008

b. Users must have a TRIM login in order to access the CNIC's TRIM dataset. Local Administrators will perform this action by using the **New Child Person** menu screen. These steps will automatically place the employee account under the correct parent organization:

- Select **Tools > Locations > All** from the menu bar to bring up all the locations.
- To find the correct organization, begin typing the name and press **Enter**.
- Right click on the organization and select **New Child Location > New Child Person**.

o General Tab

- Enter the employee's name in the **Full Name** text space.
- Select the **Full Name** button. First and last name are mandatory; do NOT complete date of birth or gender; other fields are optional.
- Select **OK**.
- Place a **check mark** in the box for **Internal**, located halfway down the form. **Note:** If you do not, the individual location icon will appear red instead of green. Green locations are visual indicators an individual or organization that is internal to your organization.

The screenshot shows a form with several fields. The 'Full Name' field is filled with 'Smith, John (Mr)'. Below it is an empty 'Address' field. Further down is a checkbox labeled 'Internal' which is checked. At the bottom, there are empty fields for 'Date of Birth' and 'Gender'.

o Electronic Addresses Tab

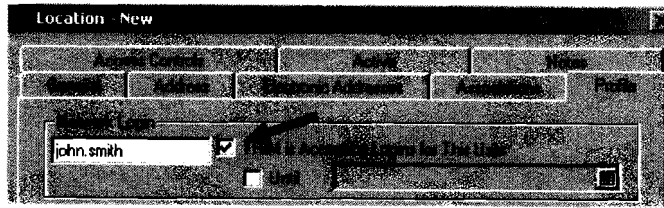
- Right click in the blank space in white box and select **new e-mail address**.
- Leave the e-mail type as Internet (for NMCI users).
- In **Address** box type the full e-mail address, i.e., john.doe@navy.mil. Select **OK**.

o Profile Tab

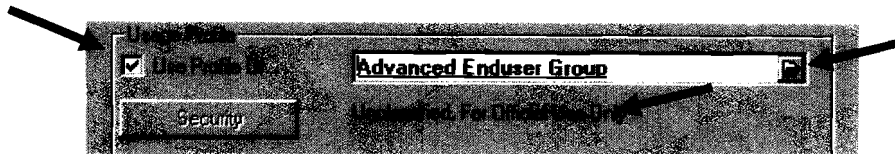
- Enter in **Network Login** the member's NMCI name, i.e., john.doe1. (**Note:** Do NOT use .ctr, .dev, or @navy.mil.)
- Select the **TRIM is Accepting Logins for This User** radio button. **Note:** If you do not put a check mark in this box, the user will not be able to access TRIM.

MAY 22 2008

- If only allowing temporary access, a termination date can be entered by checking the **Until** box and entering a date.



- Place a check mark in the **Use Profile of** and then select the User Type profile (normally the **Advanced Enduser Group** - see below 2.32 User Type).



- Select **OK**. The Security should change from (No Security Level) to Unclassified, For Official Use Only as shown above.
- Select **OK** at bottom of box and the new employee will appear under the selected parent organization.

Best Practice - An individual can belong to several locations/groups. To assign an individual to multiple locations: While in locations, right click on the **individual's name** > **Properties** > **Association** tab > **Add**. Start typing the new location and that will bring up the search box. Once the new location is found, highlight the location and click **OK**. This will add the new location in the association tab. Select **OK** to close the properties box.

Best Practice - Create or have a location to assign as an owner prior to creating record containers, folders or documents.

Best Practice - Do not assign an individual as an owner of records. Instead, assign an organization or group location to records containers, folders, and documents; then when an individual leaves, the ownership of the record does not have to change.

2-32. User Types

- a. In order to simplify the assignment of the various individual user permissions, there are four default 'User Type'

MAY 22 2008

categories for Navy datasets. Use only the developed User Type group in the **Use Profile Of** box:

- Dataset Administrator Group
- Local Administrator Group
- Power User Group
- Advanced End User Group

b. Each User Type has a different set of permissions associated with them. To view the permissions associated with each group, see below - **3-7 User Login Type Permission Table**.

c. The default user permissions will not be changed. User access rights to records and other actions in TRIM will be granted based on the User Type and the location/group an individual is associated with.

Best Practice - Access rights higher than Advanced End user, must be requested from and are only granted by the CNIC DRM.

- To request higher User Type access, e-mail the CNIC DRM, at CNIC_Records@navy.mil with the following information:
 - o Command
 - o Name of person
 - o User Type access required
 - o Reason
 - o Certification that member has completed all four training courses on NKO and is aware of the training courses available on TRIM

2-33. Groups

a. When creating groups use the group feature and end the name with the word "Group". The use of groups should be limited to special circumstances, such as: (1) when people outside the organization are working on a project/program that is not normally assigned to a given organization or, (2) the project documents/records are to be secured to a select group of people that are the only ones with permission to view and maintain the content within the container.

b. Groups cannot be associated with organizations. In other words, groups cannot be children of an organization. However, organizations can be children of a group.

MAY 22 20082-4. Security

a. Locations within TRIM are used mainly for two purposes: (1) identifying the users within the dataset and, (2) associating the user with an organization/group for security.

b. Locations should be used when access to specific containers and/or sub-folders needs to be restricted to a specific group. Security settings are not to be assigned to a given individual. Settings are only assigned by organizational location or group. When assigning access rights to a record/container, ensure the group or organizational location is used, not an individual name.

c. There are three types of locations that are essential to ensuring proper access control:

- Assignee - The current location of the record. Upon records or folder creation, the assignee of the record is based on the 'credentials' of the user logged in. For example, a user creates a record and that user is a member of N8 - Resources, then the assignee of the record will be N8 - Resources.
- Home Location - Where the record normally resides when it is not being used.
- Owner Location - Organization/department/division or position that is responsible for the record.

Best Practice - Check access or security on any type of record with a right click on the record, then select **Audit Security**.

NOTE: Access Control - The assignee of the record must be the same organization (or a child location of the organization) that is given the access controls to the record. For example, if the assignee of a record is N8 - Resources, and you change the access controls on the record to N1 - Manpower, you will receive an error message since N1- Manpower is not a child location of N8 - Resources.

2-5. Record Types - Containers/Folders/Documents. There are basically nine record types in TRIM. These record types are broken down into three types of records called boxes/containers, folders, and documents.

a. The top three levels are containers. The red container is the Command level box; the green container, called Sub-Command, can be used as a department box; and the blue

MAY 22 2008

container, called a Unit Box, can be used on the divisional level. These boxes/containers (not their contents) are viewable by everyone in the dataset.

b. Next, there are four levels of folders. Folders are where documents are filed. Use the different level of folders to sort and break down your files and documents for proper retention and disposal.

c. Finally, there are two levels for documents; however, normally only the Primary Document type will be used.

| | | | |
|--------------------|---|-----------------------|---|
| Command Box | 9 | CN-CMD-00000005 | K |
| Sub-Command Box | 8 | CN-SCB-00000041 | K |
| Unit Box | 7 | CN-UNT-00000074 | K |
| Section Folder | 6 | CN-SEC-2007-00000281 | K |
| Sub-Section Folder | 5 | CN-SSF-2007-00000295 | K |
| Work Folder | 4 | CN-WRK-2007-00000453 | K |
| Sub-Work Folder | 3 | CN-SWF-2007-00000044 | K |
| Primary Document | 2 | CN-DOC-2007-000014020 | K |
| Alternate Document | 1 | CN-ALT-2007-00000001 | K |

2-51. Title/Naming Convention. As a general rule:

a. The top three level containers should be named to identify the organization, command, department, or division.

Best Practice - Command names: The use of the command short name is authorized; HOWEVER, if in the first level container the short name is used, the full name of the command must be listed in the **Notes** tab.

Best Practice - The Command Records Manager and the CNIC DRM will determine and create the first and second level record/container structure and naming convention.

Best Practice - Departments, Divisions, and Workcenter Codes: In order to identify, throughout the dataset, which code belongs to which command, the department, division, and workcenter codes must be preceded by the command short name and followed by the noun name, i.e., CNIC N00P - Public Affairs.

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 required to be completed and describes the purpose and/or type of information that will be

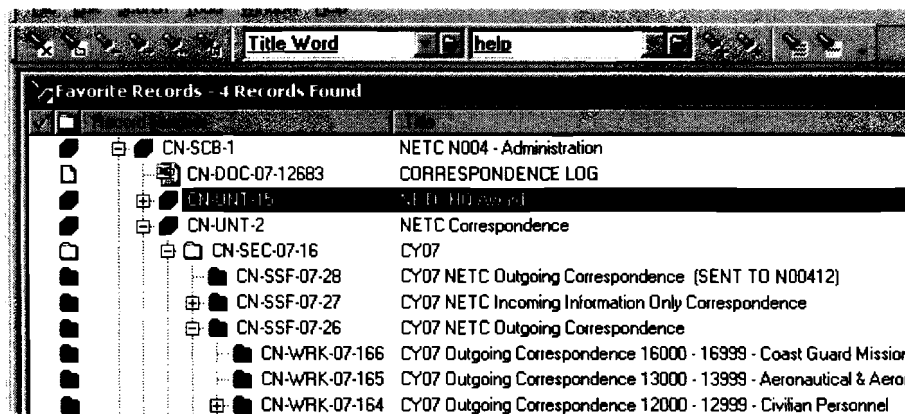
MAY 22 2008

contained in the record. Acronyms will be spelled out in the record **Notes** area.

Best Practice - Record/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.

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/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.

b. The next four levels of folders should be named to identify the type of information in the folder, i.e., fiscal or calendar year, subject area, project, program and/or business area of the folders. The example below shows a folder for CY 07 with subfolders for incoming and outgoing correspondence and then subfolders for the SSIC groups.



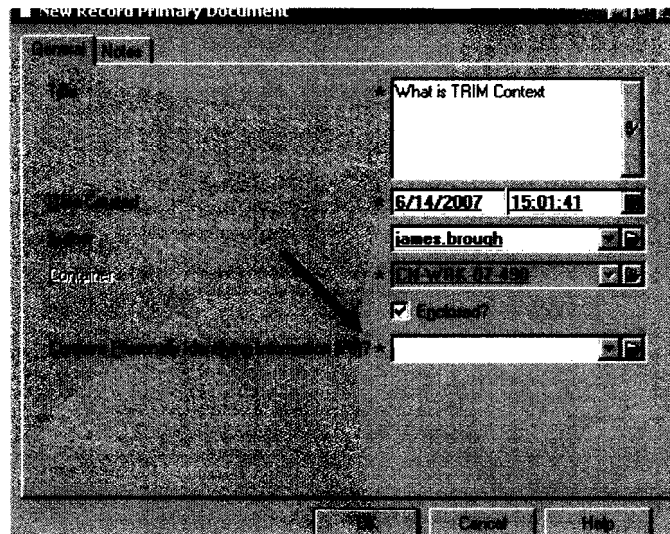
c. The document title should be sufficient to identify the subject of the document. Multiple documents in the CNIC TRIM dataset may have the same name; however, a warning will be displayed that another document in the dataset has the same title.

2-52. Creating New Documents. There are several ways to create new documents in TRIM. All of them require the same basic information in the property box. Sections with a red asterisk

MAY 22 2008

are mandatory fields and must be completed prior to checking the new document into TRIM.

NOTE: In order to identify which documents in TRIM contain Personally Identifiable Information (PII), a User Defined Field, **Contains Personally Identifying Information?**, has been added to the document check-in form and must be answered **Yes** or **No** before the document can be checked in. Documents with PII must be in a container that has location access restrictions to only users with a need to know.



- Drag and Drop. Users can select a file from another computer program and drag and drop the file onto the TRIM window or directly into the TRIM folder where it belongs.
- Document Queues. Document queues are used to move single or multiple documents from folders that reside on your local computer into a specific folder within the TRIM dataset. (See the Administrator Manual in the CNIC TRIM Help folder for setup steps.) **Note:** Ensure a time is set for searching the original folder if not automatically deleting documents from the original folder; otherwise the documents are filed multiple times in TRIM.
- Dropped Files. Similar to document queues (see below - **3-3 Moving Multiple Records into TRIM**).
- Microsoft Outlook Integration. Microsoft Outlook can be configured to integrate with TRIM. This will allow end users to catalog e-mails and/or attachments into TRIM (see below - **2-8 Outlook Integration**).

MAY 22 20082-6. Deleting Records/Documents

a. When adding an errant document or folder in TRIM, the local administrator or end user does not have the permissions to delete that document or folder. For the purpose of deleting such records, a blue "Unit box" container named "Items to be Deleted" is located under the CNIC HQ command box. All "mistakes" can be dragged and dropped by an end user into the container for the CNIC DRM to delete at a later time. The CNIC DRM is the only one with delete privileges.

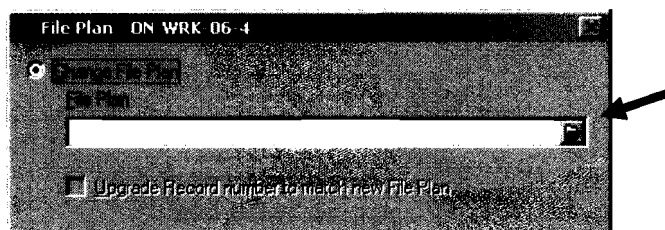
b. Documents and folders dropped into the "Items to be Deleted" box retain the security settings from their original container or folder.

Best Practice - Search for and save the "Items to be Deleted" box into the Favorite Records.

2-7. File Plan Attachment. File plans are based on Standard Subject Identification Codes (SSIC). SSICs are the single standardized system to categorize and subject classify Navy and Marine Corps information. SSICs are required on all DON records including, but not limited to, letters, messages, directives, forms, and reports regardless of format or media. Only approved SSIC codes will be assigned.

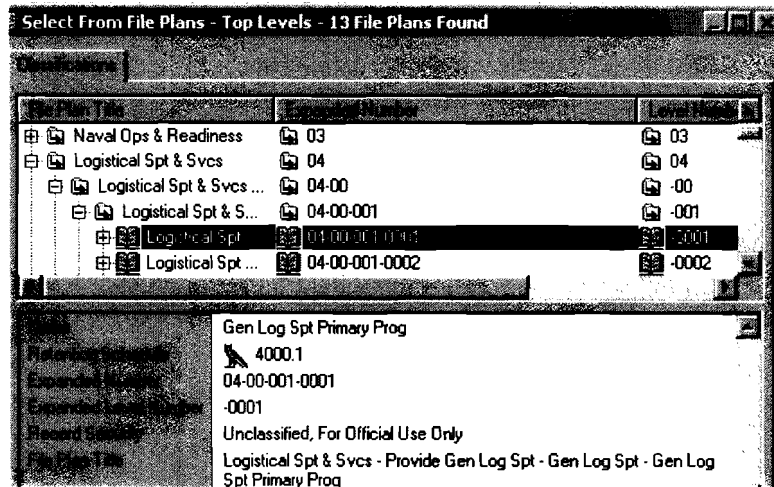
Best Practice - Proper records maintenance requires a file plan be attached to the lowest level of folders that have documents contained. All documents in the folder will have the same file plan and retention schedule.

- To attach a file plan: Right click on the appropriate folder. Select **Classify > File Plan**. Click on the "Kwik Select" icon.

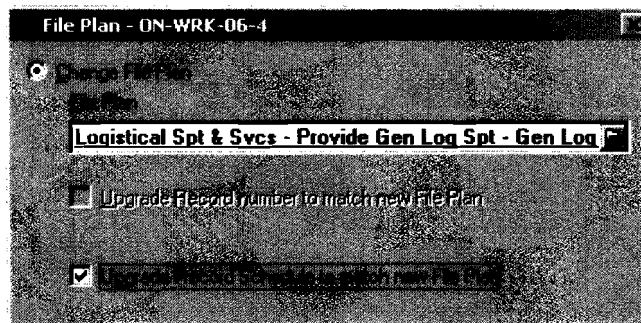


MAY 2 2 2008

- Scroll down to appropriate file plan (appropriate file plan is determined by subject area of container in which you are attaching the file plan.) > Select **OK**.



- Select **Upgrade record schedule to match new file plan**. This ensures that the associated retention schedule is applied to that record. Click **OK**.

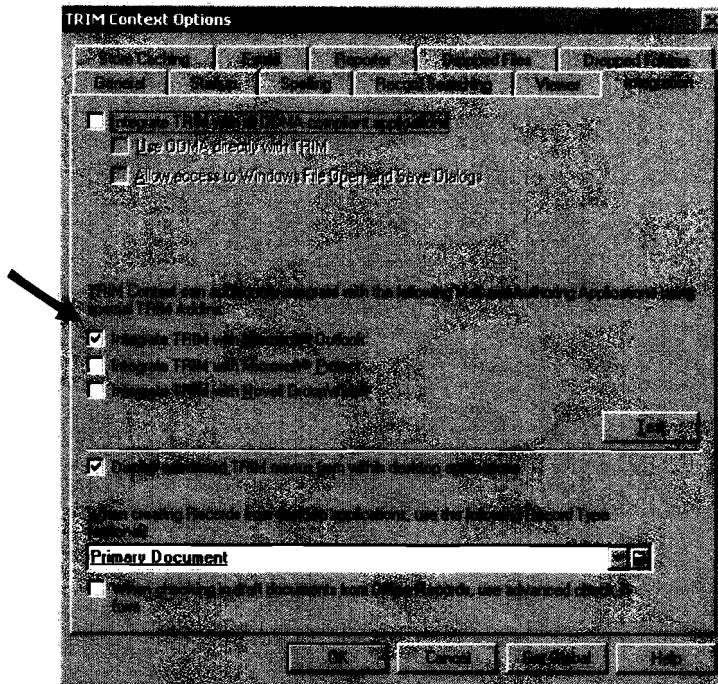


2-8. Outlook Integration

a. In order to catalog e-mails into TRIM Context from Microsoft Outlook, a few steps must first be taken to link Outlook with TRIM Context.

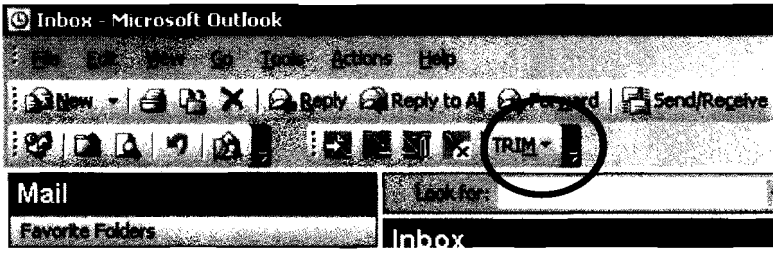
- To begin integrating TRIM with Outlook, open **TRIM > Tools > User Configuration > Options > choose Integration tab > check Integrate with Microsoft Outlook box**.

MAY 22 2008

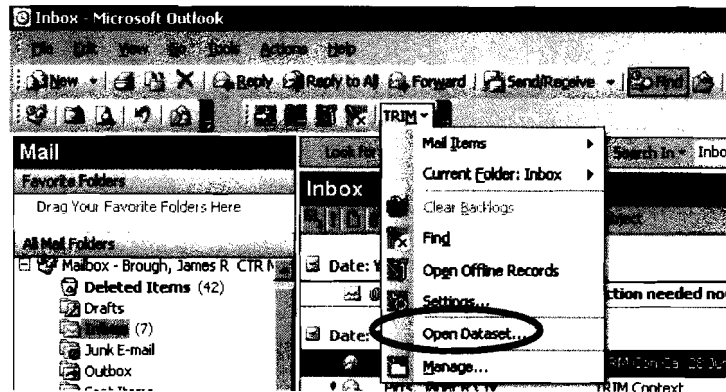


b. Once the integration options have been modified within TRIM, re-open Microsoft Outlook. You will notice that TRIM shortcut icons now appear on your Outlook toolbar.

- At this point, while in Outlook, click on the down arrow (circled below) next to TRIM on the Outlook toolbar. From the menu which appears, select the **Open Dataset** option (circled below) > **TRIM Context Dataset** screen appears, click **Add** > choose appropriate dataset **Commander, Navy Installations Command** > click **OK**. TRIM is now integrated with Microsoft Outlook.



MAY 22 2008



Best Practice - The user setting on the TRIM Outlook toolbar should be set to "Primary Record Type." Using this default will eliminate the need for the user to select the record type each time an e-mail is cataloged.

Best Practice - Storing PST files in TRIM is not authorized. The TRIM document viewer will not open PST file formats.

Best Practice - E-mail Name Changes - The local administrator should change the person's network name in the TRIM profile after the name has been changed by the e-mail administrator (NMCI).

SECTION 3 - MISCELLANEOUS

3-1. Search of Entire Dataset. Since the local administrator only has access rights to selected areas, a method is required to obtain information/records that may be controlled by other local administrators. Searches of the entire CNIC dataset will be performed by the CNIC DRM upon a written (e-mail) request to CNIC_Records@navy.mil. When a search is performed by the CNIC administrator, and a document is located which is controlled by another local administrator, permission will be requested from that local administrator to release the document to the requestor.

3-2. Edit Documents. Double clicking on a document normally opens the document in view mode.

- To edit a document - right click on the document and either choose **Edit** or **Electronic > Check Out** to make the changes.

3-3. Toolbars. There are several toolbars in TRIM to simplify the procedures a user needs most often. Users can review and select which toolbars would be most useful by:

MAY 22 2008

- Option 1: Right click anywhere in the grey area to the right of the Menu Bar and select **Navigate**.
- Option 2: Select **Tools > User Configuration > Customize > Toolbars** tab.

3-4. Removing Users With Records Checked Out

a. There will be situations when you need to remove a user who has records checked out. Some possible scenarios:

- Attempting to remove a user from the TRIM dataset and TRIM will not allow it because the individual has records checked out and they are unavailable to check the record back into the system.
- You are attempting to remove a record/document from TRIM but it will not allow you because the record is checked out to a user. (You have verified that this document has to be removed and the user is unable to check in the record.)
- The document is an urgent document and the individual who has the record is unavailable, and it has to be returned to TRIM.

b. To check in the document:

- Find the document(s) that needs to be returned.
- Right click on document > **Electronic > Check In**.
- When the Check-In form appears, you will notice that the only button available is **Discard any Modifications**. Make sure that this option is selected and select OK. This should release the record from Checked Out status.
- If the user is still a part of the command and the document was checked in as a result of the previous situation, send that individual an e-mail notifying them the record was checked in.

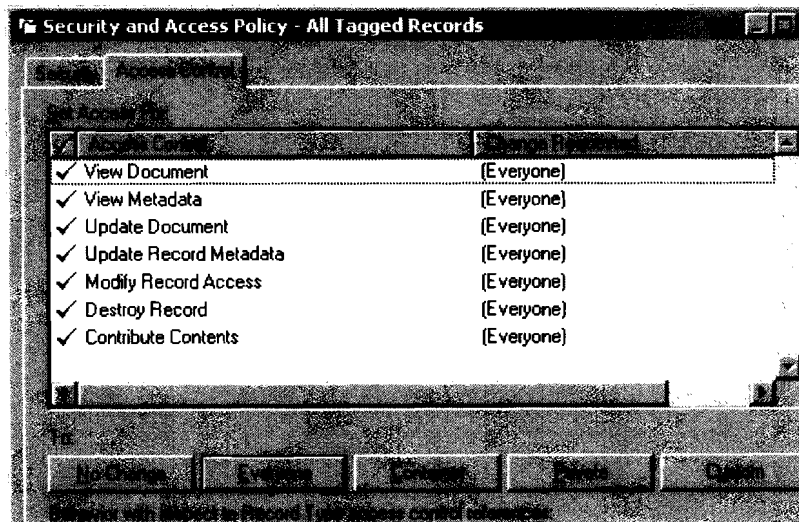
NOTE: A checked out document is stored locally on computers, normally in a subfolder under the "My Documents" folder. When a record is checked in by someone other than the person who checked out the document, the document will remain in the "My Documents" folder (with the changes, if any were made). The document can then either be deleted from the "My Documents" folder or, if permitted (meaning no one has "finalized" the record), they can check in their chop (which will be the new top copy revision of the record).

MAY 22 2008

3-5. Reassigning Owner Locations. If there is an incorrect owner location on any folder level, take the following steps to correct:

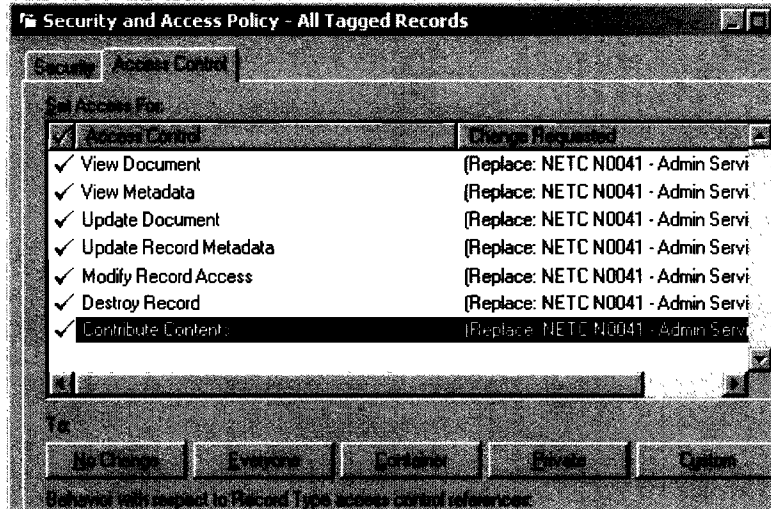
a. Multiple Records (the following show how to make several changes at one time):

- Tag appropriate records.
- Right Click. Select **Location > Owner > All Tagged Records > OK > Select Correct Location (Use Owner Location) > Yes To All**.
- Right Click. Select **Location > Assignee > All Tagged Records > OK > Select Set to Location button > Select Correct Location (Use Owner Location) > OK > Yes to All**.
- Right Click. Select **Audit/Security > Security/Access > All Tagged Records > OK > Select Access Control tab > Select Custom button > Tag all six access controls (you will see the "change requested" column change to Everyone) > OK**.
- Right Click. Select **Audit/Security > Security/Access > All Tagged Records > OK > Select Access Control tab > Select Custom button > Ensure Appropriate Organization is selected (Use Owner Location) > Tag each of the six access controls (as you did in step four; you will see the "Change Requested" column change to Organization you have selected) > OK**.
- When all steps are completed, un-tag records.



(Before Change)

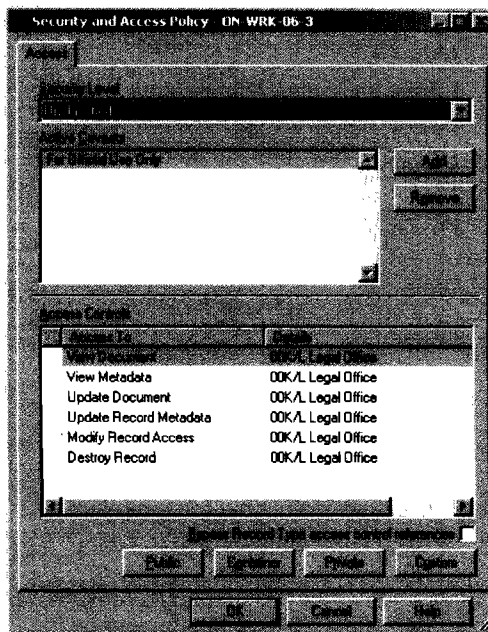
MAY 22 2008

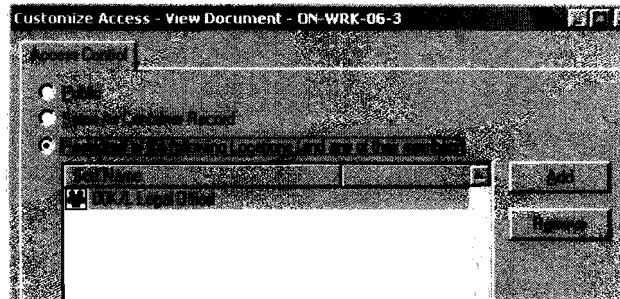


(After Change)

b. Single Record:

- Select the appropriate record.
- Right Click. Select **Location** > **Owner** > Select Correct Owner Location > **OK**.
- Right Click. Select **Location** > **Assignee** > Select Correct Assignee (Owner Location) > **OK**.
- Right Click. Select **Audit/Security** > **Security/Access** > Tag all six access controls listed in the Access Controls section > **Custom** > Select "**Restricted to the following Locations**" button > Remove wrong organization > Add appropriate owner location > **OK**.

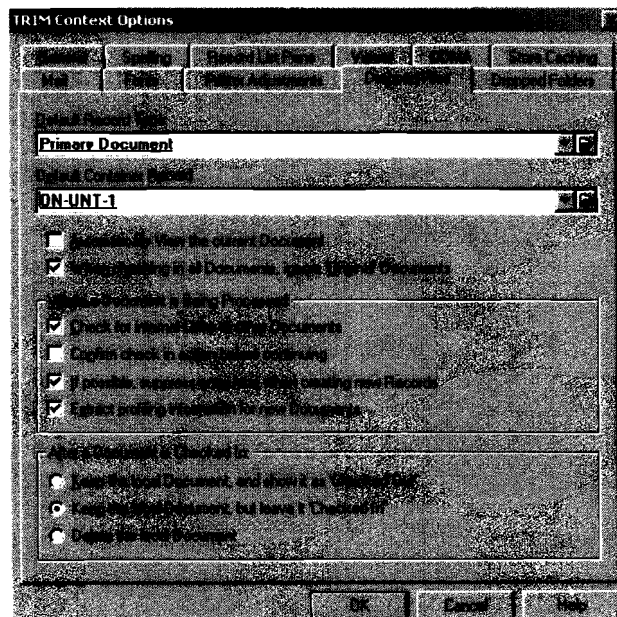


MAY 22 2008

3-6. Dropped Files - Moving Multiple Documents into TRIM.

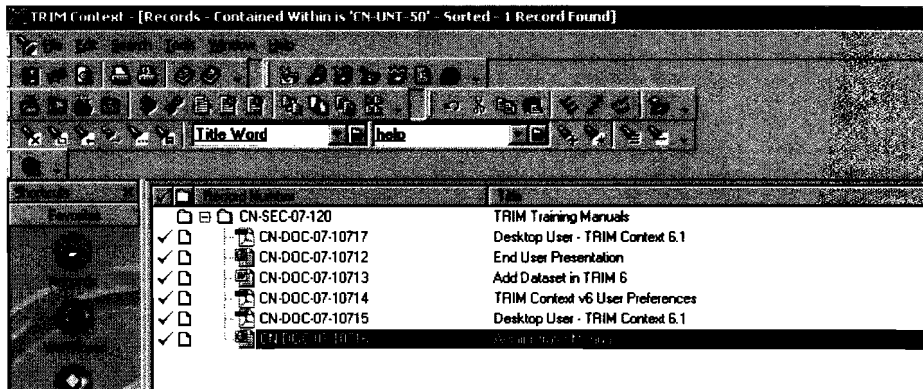
Individual records can be moved into TRIM by the drag and drop method as outlined in the end user guide. However, if you have multiple records that need to be moved from a single location to a single location in TRIM, the Dropped Files method can be used as outlined below.

- From the Command Bar, select **Tools > User Configuration > Options** and then select the **Dropped Files** tab.
- In the **Dropped Files** tab, select data for the following fields. **Note:** The following are mandatory fields:
- **Default Record Type** > Select **Primary Document** from the Kwik select.
- **Default Container Record** > Use the pulldown arrow or Kwik select to find the **container** where the documents need to reside. **Note:** Unless this setting is changed, this is where all the documents will reside when dragged into the grey area within TRIM.
- Click **OK**.



MAY 22 2008

- Navigate to your hard drive or shared drive (wherever the documents are located) and select/highlight the documents you want to move.
- Drag the documents into the grey space in TRIM. **Note:** Any open windows in TRIM should be closed.
- Tag the records by clicking on them in the checkbox column or right click and select **Tag All**.



- Right click and select **Check-In**.
- The documents will now exist in TRIM. To view the documents, conduct a search by "Date Registered" or simply navigate to the container. (**Note:** For all future dropped files, you must change the location of the documents if they should be stored elsewhere.)

3-7. User Login Type Permission Table

| TRIM Record Update Permissions | Login Type | | | |
|------------------------------------|-----------------------------|---------------------------|------------------|-------------------------|
| | Dataset Administrator Group | Local Administrator Group | Power User Group | Advanced End User Group |
| Create Records | Yes | Yes | Yes | Yes |
| Modify Records | Yes | Yes | Yes | Yes |
| Delete Records | Yes | No | No | No |
| Reverse Final Declaration | Yes | No | No | No |
| Create New Parts | Yes | Yes | Yes | No |
| Modify Record Class | Yes | Yes | No | No |
| Manage Requests | Yes | Yes | Yes | No |
| Record Administration | Yes | Yes | No | No |
| Record Administration (Restricted) | Yes | No | No | No |
| Record Archivist | Yes | Yes | No | No |

MAY 22 2008

| TRIM Record Update Permissions | Login Type | | | |
|----------------------------------|-----------------------------|---------------------------|------------------|-------------------------|
| | Dataset Administrator Group | Local Administrator Group | Power User Group | Advanced End User Group |
| Document Update | Yes | Yes | Yes | Yes |
| Document Delete/Purge | Yes | No | No | No |
| Append to Existing Notes | Yes | Yes | Yes | Yes |
| Can Save Record Searches | Yes | Yes | Yes | Yes |
| Add Record Relationships | Yes | Yes | Yes | Yes |
| Remove Record Relationships | Yes | Yes | Yes | Yes |
| Attach Contacts | Yes | Yes | Yes | Yes |
| Remove Contacts | Yes | Yes | Yes | Yes |
| Set Container | Yes | Yes | Yes | Yes |
| Change Container | Yes | Yes | Yes | Yes |
| Remove from Container | Yes | Yes | Yes | Yes |
| Modify Record Security | Yes | Yes | No | No |
| Set Record Archive Dates | Yes | Yes | Yes | No |
| Document Assembly Administration | Yes | Yes | No | No |
| Create Communications | Yes | No | No | No |
| Manage Communications | Yes | No | No | No |

| TRIM Location Update Permissions | Login Type | | | |
|--|-----------------------------|---------------------------|------------------|-------------------------|
| | Dataset Administrator Group | Local Administrator Group | Power User Group | Advanced End User Group |
| Can Create Internal Locations | Yes | Yes | No | No |
| Can Modify Internal Locations | Yes | Yes | No | No |
| Limited Modification of Internal Locations | Yes | No | No | No |
| Can Delete Internal Locations | Yes | Yes | No | No |
| Can Create External Locations | Yes | Yes | Yes | Yes |
| Can Modify External Locations | Yes | Yes | Yes | Yes |
| Can Delete External Locations | Yes | Yes | Yes | No |
| View User Profile Details | Yes | Yes | No | No |
| Modify Logins and User Profiles | Yes | Yes | No | No |

MAY 22 2008

| TRIM Control File Update Permissions | Login Type | | | |
|--------------------------------------|-----------------------------|---------------------------|------------------|-------------------------|
| | Dataset Administrator Group | Local Administrator Group | Power User Group | Advanced End User Group |
| Record Types | Yes | No | No | No |
| Lookup Sets | Yes | No | No | No |
| User Defined Fields | Yes | No | No | No |
| File Plan (Classifications) | Yes | Yes | No | No |
| Schedules | Yes | No | No | No |
| Holds | Yes | No | No | No |
| Spaces | Yes | Yes | No | No |
| Document Stores | No | No | No | No |
| Indexed Words | Yes | No | No | No |
| Postal Codes | Yes | No | No | No |
| Thesaurus Terms | Yes | Yes | No | No |
| Saved Searches | Yes | Yes | No | No |
| Meetings | Yes | No | No | No |
| Security Guide Entries | Yes | No | No | No |
| E-mail Templates | Yes | No | No | No |
| Data Cleanup | Yes | No | No | No |

| TRIM Workflow/Action Tracking | Login Type | | | |
|--|-----------------------------|---------------------------|------------------|-------------------------|
| | Dataset Administrator Group | Local Administrator Group | Power User Group | Advanced End User Group |
| Workflow Administration | Yes | Yes | No | No |
| Actions Administrator | Yes | Yes | No | No |
| Attach Actions or Activities | Yes | Yes | Yes | Yes |
| Reassign Actions or Activities | Yes | Yes | Yes | Yes |
| Reschedule Actions | Yes | No | No | No |
| Complete Actions or Activities | Yes | Yes | Yes | Yes |
| Create Workflow | Yes | Yes | Yes | Yes |
| Create Workflow Without Using Template | Yes | Yes | Yes | No |
| Modify Workflow | Yes | Yes | Yes | No |

MAY 22 2008

| TRIM Miscellaneous Permissions | Login Type | | | |
|-------------------------------------|-----------------------------|---------------------------|------------------|-------------------------|
| | Dataset Administrator Group | Local Administrator Group | Power User Group | Advanced End User Group |
| Reporter Administrator | Yes | Yes | No | No |
| Run Statistics | Yes | Yes | Yes | No |
| Edit Business Calendar | Yes | Yes | No | No |
| Change System Settings | Yes | No | No | No |
| Use Caption Editor | Yes | Yes | No | No |
| Security and Audit Administrator | Yes | No | No | No |
| Define Barcode Scanners | Yes | Yes | Yes | No |
| Define Web Templates | Yes | Yes | Yes | No |
| Bypass View Access Controls | Yes | No | No | No |
| Bypass All Access Controls | Yes | No | No | No |
| Import And Export | Yes | No | No | No |
| Bypass Lockdown | Yes | No | No | No |
| Run SQL Queries in SDK Applications | Yes | Yes | No | No |

| TRIM Location Usage Permissions | Login Type | | | |
|--------------------------------------|-----------------------------|---------------------------|------------------|-------------------------|
| | Dataset Administrator Group | Local Administrator Group | Power User Group | Advanced End User Group |
| Can be Record Home | Yes | Yes | Yes | Yes |
| Can be Record Owner | Yes | Yes | Yes | Yes |
| Can be Record Assignee | Yes | Yes | Yes | Yes |
| Can be Record Contact | Yes | Yes | Yes | Yes |
| Can be Record Requestor | Yes | Yes | Yes | Yes |
| Can be Action/Activity Assignee | Yes | Yes | Yes | Yes |
| Can be Activity Supervisor | Yes | Yes | Yes | No |
| Can be Assigned to an Access Control | Yes | Yes | Yes | Yes |

MAY 22 2008

**RECORDS MANAGEMENT REVIEW CHECKLIST
SELF-EVALUATION CHECKLIST**

| | |
|-------------------|-----------------|
| Organization: | |
| Location: | |
| Date Initiated: | Date Completed: |
| Action Officer: | |
| | |
| Telephone Number: | |
| Reviewer: | |

PART I - REQUIRED REFERENCES

- | | <u>YES</u> | <u>NO</u> |
|--|--------------------------|--------------------------|
| 1. SECNAVINST 5210.8D, DON Records Management Program, of 31 December 2005. ON HAND | <input type="checkbox"/> | <input type="checkbox"/> |
| 2. SECNAVINST 5216.5D, DON Correspondence Manual, of 29 August 1996 with Changes 1 and 2. ON HAND | <input type="checkbox"/> | <input type="checkbox"/> |
| 3. SECNAV M-5210.1, DON Records Management Manual, of 31 December 2005. ON HAND | <input type="checkbox"/> | <input type="checkbox"/> |
| 4. SECNAV M-5210.2, DON Standard Subject Identification Codes, of 31 December 2005. ON HAND | <input type="checkbox"/> | <input type="checkbox"/> |
| 5. CNIC TRIM Best Practice Guide, October 2007. ON HAND | <input type="checkbox"/> | <input type="checkbox"/> |

PART II - RECORDKEEPING REQUIREMENTS AND DISPOSITION STANDARDS

Ensuring adequacy of documentation in any information system depends on the clear articulation of recordkeeping requirements. Recordkeeping requirements specify the creation and maintenance of specific records to document DON operations and activities, facilitate action by DON officials and their successors, permit continuity and consistency in administration, make possible a proper scrutiny by Congress and other duly authorized agencies, protect the rights of the Government and those affected by its actions, and document important meetings and the formulation and implementation of basic policy and decisions.

MAY 22 2008

FILING PROCEDURES

- | | <u>YES</u> | <u>NO</u> |
|---|--------------------------|--------------------------|
| 1. Are files centrally managed within the command/department? (SECNAV M-5210.2, Chapter 1, paragraph 2a) Remarks: | <input type="checkbox"/> | <input type="checkbox"/> |
| <hr/> | | |
| 2. Is a person assigned the responsibility to coordinate all command/department files? (SECNAV M-5210.2, Chapter 1, paragraph 2a(1)) Remarks: | <input type="checkbox"/> | <input type="checkbox"/> |
| <hr/> | | |
| 3. Is there a file plan listing the file numbers, titles, and disposition for each record series maintained in the section? (SECNAV M-5210.2, Chapter 1, paragraph 2c) Remarks: | <input type="checkbox"/> | <input type="checkbox"/> |
| <hr/> | | |
| 4. Does the command/department have a Vital Records Plan, and have vital records been identified? If so, is the plan reviewed annually? (SECNAV M-5210.2, Chapter 1, paragraph 3) Remarks: | <input type="checkbox"/> | <input type="checkbox"/> |
| <hr/> | | |
| 5. Is there a procedure for keeping track of documents removed from the files? (SECNAV M-5210.2, Chapter 1, paragraph 4) Remarks: | <input type="checkbox"/> | <input type="checkbox"/> |
| <hr/> | | |
| 6. Have cut-off dates (general correspondence files at the end of each calendar year, and budget and accounting files at the end of each fiscal year) been established? (SECNAV M-5210.1, Chapter 1, paragraph 5, and SECNAV M-5210.1, Part 1, paragraph 11a(1)) Remarks: | <input type="checkbox"/> | <input type="checkbox"/> |

MAY 22 2008

| | <u>YES</u> | <u>NO</u> |
|--|--------------------------|--------------------------|
| 7. Are case files closed when action has been completed or upon the occurrence of a particular event or action? (SECNAV M-5210.2, Chapter 1, paragraph 5, and SECNAV M-5210.1, Part 1, paragraph 11a(2)) | <input type="checkbox"/> | <input type="checkbox"/> |

Remarks:

| | | |
|---|--------------------------|--------------------------|
| 8. Is disposal control guidance for each record series posted on file cabinets, drawers, guides, or file folders as appropriate? (SECNAV M-5210.1, Part II, paragraph 6d) | <input type="checkbox"/> | <input type="checkbox"/> |
|---|--------------------------|--------------------------|

Remarks:

| | | |
|--|--------------------------|--------------------------|
| 9. Are non-current (cut off) or terminated files moved to a lower file drawer or to other less convenient office space? (SECNAV M-5210.1, Part I, paragraph 11b) | <input type="checkbox"/> | <input type="checkbox"/> |
|--|--------------------------|--------------------------|

Remarks:

| | | |
|---|--------------------------|--------------------------|
| 10. Are personal papers clearly marked and filed separately from the official records of the office? (SECNAV M-5210.1, Part I, paragraph 14b) | <input type="checkbox"/> | <input type="checkbox"/> |
|---|--------------------------|--------------------------|

Remarks:

| | | |
|--|--------------------------|--------------------------|
| 11. Are electronic records saved in the DON approved electronic recordkeeping system (i.e., TRIM)? (SECNAV M-5210.1, Part I, paragraph 17) | <input type="checkbox"/> | <input type="checkbox"/> |
|--|--------------------------|--------------------------|

Remarks:

MAY 22 2008

RECORDS DISPOSAL PROGRAM

| | <u>YES</u> | <u>NO</u> |
|---|--------------------------|--------------------------|
| 12. Are inactive records retired to a local records center or the Federal Records Center in accordance with the policies prescribed in SECNAV M-5210.1, Part I, paragraph 7a? | <input type="checkbox"/> | <input type="checkbox"/> |

Remarks:

| | | |
|--|--------------------------|--------------------------|
| 13. Are records disposed of annually in accordance with the disposal guidance contained in Part III of SECNAV M-5210.1? (SECNAV M-5210.1, Part I, paragraphs 1h and 2) | <input type="checkbox"/> | <input type="checkbox"/> |
|--|--------------------------|--------------------------|

Remarks:

| | | |
|---|--------------------------|--------------------------|
| 14. Are records not covered by the retention standards in Part III of SECNAV M-5210.1 retained and reported to the Command Records Officer and CNO (DNS-5)? (SECNAV M-5210.1, Part II, paragraph 4) | <input type="checkbox"/> | <input type="checkbox"/> |
|---|--------------------------|--------------------------|

Remarks:

| | | |
|---|--------------------------|--------------------------|
| 15. Is an annual inspection and review of local disposal procedures for the activity's records conducted to ensure that records disposal and retention procedures are current, adequate, understood, and applied regularly and effectively; and proper retention standards have been applied to all records accumulated? (SECNAV M-5210.1, Part II, paragraph 5d) | <input type="checkbox"/> | <input type="checkbox"/> |
|---|--------------------------|--------------------------|

Remarks:

| | | |
|---|--------------------------|--------------------------|
| 16. Are incidents where records are accidentally destroyed reported to CNO (DNS-5) or for the Marines, to CMC (ARDB)? (SECNAV M-5210.1, Chapter 1, paragraph 6) | <input type="checkbox"/> | <input type="checkbox"/> |
|---|--------------------------|--------------------------|

Remarks:

MAY 22 2008

| | <u>YES</u> | <u>NO</u> |
|--|--------------------------|--------------------------|
| 17. Are the procedures described in SECNAV M-5210.1, Appendix A, used to retire records to the Federal Records Center? (SECNAV M-5210.1, Part 1, paragraph 1a) | <input type="checkbox"/> | <input type="checkbox"/> |

Remarks:

| | | |
|---|--------------------------|--------------------------|
| 18. Are records that the National Archives appraised as "Permanent" in parts III, IV and V of SECNAV M-5210.1 transferred to the National Archives and Records Administration as prescribed in the records' disposition guidance? (SECNAV M-5210.1, Part 1, paragraph 7b) | <input type="checkbox"/> | <input type="checkbox"/> |
|---|--------------------------|--------------------------|

Remarks:

PART III - TRIM IMPLEMENTATION

| | <u>YES</u> | <u>NO</u> |
|--|--------------------------|--------------------------|
| 19. Is there a command/departmental TRIM Local Administrator assigned and aware of their responsibilities and duties? (CNIC TRIM Best Practice Guide, paragraph 1.5) | <input type="checkbox"/> | <input type="checkbox"/> |

Remarks:

| | | |
|---|--------------------------|--------------------------|
| 20. Are all members of the command/department able to log into the CNIC dataset? (CNIC TRIM Best Practice Guide, paragraph 2.2) | <input type="checkbox"/> | <input type="checkbox"/> |
|---|--------------------------|--------------------------|

Remarks:

| | | |
|--|--------------------------|--------------------------|
| 21. Is the command/department using TRIM for Electronic Records Management? (CNIC TRIM Best Practice Guide, paragraph 1.6) | <input type="checkbox"/> | <input type="checkbox"/> |
|--|--------------------------|--------------------------|

Remarks:

MAY 22 2008

22. Are sufficient folders created for document filing and disposition? (CNIC TRIM Best Practice Guide, paragraph 2.5) YES NO

Remarks:

23. Are disposition File Plans attached to the lowest level of folders? CNIC TRIM Best Practice Guide, paragraph 2.7)

Remarks:

UNCLASSIFIED

ACTION MEMO

19 Mar 07

From: Mr.  Harry Olson, Director, Command and Staff
To: Commander, Navy Installations Command

SUBJECT: CNIC, RECORDS MANAGEMENT PROGRAM

- Approve instruction as outlined in TAB A and post to CNIC portal directives.
- Cost: N/A
- TAB A establishes policies to ensure administrative information created or acquired by activities and offices is properly managed from creation/receipt through final disposition.

RECOMMENDATION: Sign TAB A

ATTACHMENTS: As stated

Prepared By: Anthony Schlim, CNIC Records Manager, 19 Mar 08

Route By: Anthony Schlim, CNIC Records Manager, 19 Mar 08