

Corporate and Service Node User's Guide

February 2012, Version 5.9

TRICARE Management Activity

Business and Economic Analysis Division

Revision History

Version	Date	Description of Changes
3.2.2	11 Oct 2002	<ul style="list-style-type: none"> • Base Version.
3.2.3	09 Jan 2003	<ul style="list-style-type: none"> • Altered Updates Frequency Table to reflect SADR weekly updates. • Revised Appendix A, Section 3 to reflect changes on Checkpoint website.
4.0	28 Mar 2003	<ul style="list-style-type: none"> • Altered language to present tense. • Added Corporate Node HPAE/Axiom File system. • Added Lead Agents File systems. • Revised to reference Bill Pierce as Corporate Node Administration Staff. • Revised Appendix A, Section 5 to reflect WinSCP v2.2 changes. • Revised Appendix A, Section 12 to include 'chmod' instructions. • Added CHAMPUS DRG Version to Appendix F, Section 4. • Revised Appendix A, Sections 3 & 4 to remove VPN Telnet. • Revised Appendix A, Section 4/5 to remove VPN FTP. • Revised Appendix A, Section 6 to include Password Variables in SAS. • Added Appendix A, Section 12: Changing Your OKC SP Password.
4.1	15 Apr 2003	<ul style="list-style-type: none"> • Update Appendix B with current data and naming conventions • Add date field to Import and Export Transmittals
4.1.1	01 May 2003	<ul style="list-style-type: none"> • Add Dr. Guerin as Functional Manager & Access Authority for Lead Agent – Europe
4.1.2	15 May 2003	<ul style="list-style-type: none"> • Update MDR Information • Added 1TB for Corporate Node • Updated AIX version from 4.3.3 to 5.1 • Removed file system space allocation • Added Army Service Node information
4.1.3	19 May 2003	<ul style="list-style-type: none"> • Removed info regarding space allocations per file system - JSL. • Removed Ft. Detrick PWAF rollover statement.
4.1.4	20 May 2003	<ul style="list-style-type: none"> • Removed DRG Grouping Appendix F and references to the appendix – JSL.
4.2	28 Jul 2003	<ul style="list-style-type: none"> • Revised Guide to reference new contact info for Bill Pierce. • Revised MDR PWAF to reference HPA&E/TMA Privacy Office rather than Director, HPA&E. • Revised MDR PWAF instructions to reference TMA Privacy Office for ADP & Data Use Agreements. • Altered Section X., Node Separation & Overhead to include "at a minimum". • Appendix A, Section 15: Resource Consideration: removed note re: total disk space. • Removed Chaya Merrill's name and replaced with Linda Cottrell.
4.2.1	7 Aug 2003	<ul style="list-style-type: none"> • Revised VPN for IKE (not FWZ)
4.2.2	29 Sep 2003	<ul style="list-style-type: none"> • Revised/Updated PuTTY & WinSCP instructions • Updated Corporate & Service Nodes file systems • Added Appointment Data
4.2.3	6 Nov 2003	<ul style="list-style-type: none"> • Added mdata command for viewing MDR metadata • Removed section describing moving files from Ft. Detrick to SCE • Added MCFAS & SOC to data types in file naming conventions • Removed Bill Pierce as SCE Administrator • Removed Linda Cottrell as STI authority
4.2.4	8 Jan 2004	<ul style="list-style-type: none"> • Added Tom Davy as STI authority
4.2.5	16 Jan 2004	<ul style="list-style-type: none"> • Updated metadata section • Added Corporate Node /rm/Altarum file system
4.2.6	5 Apr 2004	<ul style="list-style-type: none"> • Removed Martin Shepherd as Altarum functional authority • Added Lockheed Martin file system and authority • Replaced Don Ward with Richard Bannick as /rm/altarum authority • Added Privacy Act and HIPAA information for using/storing files • Updated file naming conventions – new SAS data sets, NED data, etc • Updated WinSCP download directions for new version • Updated SecuRemote download directions
4.2.7	13 Apr 2004	<ul style="list-style-type: none"> • Updated Storing and Securing Privacy Act Data section
4.2.8	4 May 2004	<ul style="list-style-type: none"> • Updated directions for using mdata
4.2.9	12 May 2004	<ul style="list-style-type: none"> • Updated functional authority for Altarum

Version	Date	Description of Changes
4.3.	November 2004	<ul style="list-style-type: none"> • Added Tom White as Altarum authority • Removed Tom Davy as STI authority • SAS Work Space Corporate Node (small, medium & large) • SAS 8.2 & 9.12 on both Corporate & Service Nodes • SAS Work Space Service Node (small & large) • Updated WinSCP download to include loading an updated version over an outdated version, or a new install • Updated PuTTY download to include loading an updated version over an outdated version, or a new install • New dental data type added to MDR (MMSO) • Chron Job 'at' function • SAS temp work space residual aborted data will be deleted by DHSS • Renamed from SCE to Corporate and Service User's Guide • Navy BUMED POC • Added STI: Lily Grimm • CASS 30 day migration rule • New Casualty Data • New Master Death File Data • New Encounter Death Data • New DEERS VM4 Data • Change Telnet to SSH for changing passwords
4.3.1.	January - May 2005	<ul style="list-style-type: none"> • New MEPRS Ancillary Data, Contains Ancillary Procedures found in MEPRS • New Appointment Data • New Designated Provider (clinical) Data • New Designated Provider (pharmacy) Data • New Designated Provider (provider) Data • New Enrollment Norms File • Altarum Director, TMA RM, Mr. Tom White replaces Dr. Richard Bannick • Revised password instructions (must be 8 characters) • New Reservist Data • Anticipated Ancillary Data • Revised MDR access form
4.3.2	June – Sept 2005	<ul style="list-style-type: none"> • New Longitudinal VM4 Data (LVM4) • Updated the SecuRemote VPN details.
4.3.3	September 2005	<ul style="list-style-type: none"> • Submitting SAS Job using accounting codes • Air Force added to Service Node
4.4.	Dec 2005- April 2006	<ul style="list-style-type: none"> • New TED Institutional Data • Ancillary Data • CSS removed • Removed Lily Grimm as authority for STI • Corporate Project Accounting Code
4.5	April – June 2006	<ul style="list-style-type: none"> • Updated VPN instruction set
4.5.1	July – August 2006	<ul style="list-style-type: none"> • Updated password section • New TED Provider Data (TEDPR) • Anticipated TED Non-institutional Data • Updated export transmittal form
4.5.2	Sept – Oct 2006	<ul style="list-style-type: none"> • Updated HSM Tables E-1A through E-3 • Updated Table 2 Update Frequency Per Data Type • Added VM6 Data Types throughout document
4.5.3	Nov 06 – March 2007	<ul style="list-style-type: none"> • Removed SecuRemote VPN install instructions • Added NetScreen VPN install • Added SecuRemote VPN uninstall
4.5.4	Aug 2008	<ul style="list-style-type: none"> • Included information about new DD 2875 form with instructions from DHSS
4.5.5	Nov 2008	<ul style="list-style-type: none"> • Remove VPN client details from manual • Add new password change steps • Instructions for the OOB • Rework WINscp to include new IP addresses • Rework PuTTY to include new IP addresses • Remove midsas instructions

Version	Date	Description of Changes
		<ul style="list-style-type: none"> • Update sas and bigsas instructions • Special Justification Form Example (Appendix G) • Included screen shots of the DD2875 form • Rename EIDS to DHSS
4.5.6	Dec 2008	<ul style="list-style-type: none"> • Included Juniper Host Checker details from DISA OKC • Updated most screen shots to ensure OKC IP's present • Map Corp Node II file systems to Corp Node in OKC • Updated sponsor allocated file systems • Updated data file systems in pub
4.7	March 2009	<ul style="list-style-type: none"> • Removed SOC from data types in file naming conventions, part of reservist file • Revised file system location of DEERS data types • OKC DISA Juniper Tool Updates (Removing Juniper 6.0 and installing Juniper 6.3 VPN) • Collapse SADR Quarter data into Fiscal Year
4.7.1	June 2009	<ul style="list-style-type: none"> • Revised data extraction instructions • Revised export transmittal
4.8	August 2009	<ul style="list-style-type: none"> • Revised Juniper OOB SSL VPN sign-on instructions • Revised WinSCP for Secure File Transfer instructions • Updated Access Authority for SRA under Sponsor Allocated File Systems • Revised overall Table of Contents to link to sections • Revised Appendix A Table of Contents to hyperlink to sections • Revised Appendix B Table of Contents to hyperlink to sections • Revisions of content and formatting to make document more user friendly
4.9	October 2009	<ul style="list-style-type: none"> • Included updated DD2875 form as well as the DISA link to the interactive PDF
5.0	December 2009	<ul style="list-style-type: none"> • Updated instructions on the use of PKZIP • Updated instructions for the DoD Information Assurance Awareness certificate (formerly called Security Awareness) • Removed Accessing the DISA SSL VPN at the end of the document as redundant (see section A-3)
5.1	January 2010	<ul style="list-style-type: none"> • Included SAS macro for saving SAS logs for HIPAA compliance under "Keeping Logs" • Included instructions for filling out the MDR AARF • Removed listing of corporate and service node file system listings and modified language in those sections • Removed Job Accounting section
5.2	March 2010	<ul style="list-style-type: none"> • Updated instructions for form DD2875 and the link to the form • Removed the imbedded form DD2875 and referred to link instead
5.3	April 2010	<ul style="list-style-type: none"> • Updated security guidelines for strong passwords in Section A-12 • Updated contact information for password reset in Section A-12 • Updated various data types available • Updated Juniper OOB SSL VPN instructions • Indicated metadata command no longer working • Removed Appendix F. How to access the DISA DECC OKC SAS Corporate and Service Nodes and renamed subsequent appendices • Removed instructions for running SAS 8 (no longer available)
5.4	June 2010	<ul style="list-style-type: none"> • Updated rules for Storing and Securing Privacy Act Data
5.5	September 2010	<ul style="list-style-type: none"> • Updated information and instructions in Storing and Securing Privacy Act Data • Updated instructions for DD2875 • Updated Table 3-2. Data Types in /mdr/pub • Updated and modified Section B-5: PUB Data Types • Changed instructions for changing password and contact information, Section A-12 • Moved Section B-6: Acronyms to Section B-7 • Changed Section B-6 to the listing of reference files available • Added contact information to Sections A-6 and A-7, Import and Export Transmittal Requests, respectively. • Added information to chmod command (pg 54) • Added non-OOB IP addresses for *.mil users to PuTTY for Secure Shell (SSH) Login and WinSCP for Secure File Transfer

Version	Date	Description of Changes
5.6	October 2010	<ul style="list-style-type: none"> • Clarified use of Export Transmittal request in regards to PHI data • Updated Section B-6: REF Data Types
5.7	April 2011	<ul style="list-style-type: none"> • Clarified new user password instructions on pg. 26 • Added statement on maximum number of programs submitted on pg 34 • Added information on CAPER Enhanced on pg 75 • Updated metadata access instructions in Section A-9 • Updated DD2875 instructions for including metadata access for new account requests • Included password server OOB and Non-OOB (*.mil only) IP addresses in sections A-3 and A12
5.8	July 2011	<ul style="list-style-type: none"> • Updated Section A-5 for submitting a SAS program • Changed MDR Functional Proponent for sending PHI download/upload notifications (p 16) • Updated MDR application and instructions (Appendix D) • Changed BEA reference to DHCAPE
5.9	February 2012	<ul style="list-style-type: none"> • Updated Export Transmittal form (Attachment A-2) • Updated MDR AARF (Appendix D)

Table of Contents

I.	Introduction	7
II.	Background.....	7
III.	Overview of the MDR Operating Capability Data Sets.....	7
IV.	System Overview and Technical Architecture	9
V.	System Functionality.....	9
VI.	System Operations	10
VII.	Overview of Access Requirements.....	12
VIII.	User Support, Training and Documentation	13
IX.	System Server Administration	13
X.	Space Allocation and Related Issues	14
	Appendix A. Basic User's Guide for UNIX and SAS.....	18
	Appendix B. MDR File Naming Conventions for the Corporate and Service Nodes	66
	Appendix C. Load Leveler and Computing Resource Management.....	90
	Appendix D. Corporate or Service Node Access and Security Requirements	93
	Appendix E. Hierarchical Storage Management (HSM)	105
	Appendix F. Special Justification Example	108
	Appendix G. DISA TOOLS.....	110

I. Introduction

The Corporate and Service Nodes provide authorized individuals with access and query capability to specified Military Health System (MHS) Data Repository (MDR) data sets. The Corporate and Service Nodes are an extension of the existing Defense Health Services Systems (DHSS) architecture and do not add additional data elements, file types, or functionality beyond that offered by the existing DHSS product suite. This User Guide addresses the processes for accessing and utilizing the Corporate and Service Nodes.

II. Background

The Corporate and Service Nodes replaced reporting and data analysis capabilities lost with the termination of computing services at Fort Detrick. Extension of the existing DHSS architecture satisfied this requirement.

III. Overview of the MDR Operating Capability Data Sets

Data sets contained within the MDR include workload, cost, population, enrollment, demographic, and reference data for the MHS. The data sets are arrayed in a structured manner. They are available post processing and are represented as a subset of the MDR file catalogue:

- According to a defined periodicity or update cycle;
- Processed using known, tested software - with identified business rules;
- Quality controlled, documented, and reviewed; and
- Released for specified use.

MDR Data Sets

Data Content:

MTF Clinical System Data

- Direct Care Encounter Data (*Standard Ambulatory Data Record, SADR*)
- Direct Care Encounter Data (*Comprehensive Ambulatory/Provider Encounter Record, CAPER*), Basic and Enhanced
- Direct Care Inpatient Data (*Standard Inpatient Data Record, SIDR*)
- Worldwide Workload Report Data (*WWR*)
- Completion Factor Data (*SADR CompFac and SIDR CompFac*)
- Appointment Data (*APPT*)
- Ancillary (ANCIL) Laboratory and Radiology
- Referral Data
- Case Management

Manpower, Workload, Expense Data

- MEPRS Executive Query System (*MEQS*) (Archival – 1996-2001 Only)
- Expense Assignment System (*EAS-IV*)

Beneficiary Demographics Data

- Point-in-time Extract Data (*PITE*) (Archival Only)

- Population Summaries (*PITE-AGG*) (Archival Only)
- Enrollment Data (*TRICARE Enrollment File*) (Archival Only)
- Enrollment Summaries (*Longitudinal Enrollment File*) (Archival Only)
- Non-Availability Statement (*NAS*) Aggregate & Beneficiary (Archival – 1994-2001 Only)
- DEERS VM
- Longitudinal Enrollment (*LVM*, replaced by Longitudinal Eligibility)
- Longitudinal Eligibility (*LELG*)
- Reservist (*Reservist*)
- Managed Care Forecasting and Analysis System (*MCFAS*)

Centralized Pharmacy Data

- Pharmacy Data Transaction Service (*PDTS*)
- National Mail Order Pharmacy data (*NMOP*)

Purchased Care Data

- TRICARE Encounter Data – Institutional Data (*TEDI*)
- TRICARE Encounter Data – Provider Data (*TEDPR*)
- TRICARE Encounter Data – Non-institutional Data (*TEDNI*)
- Health Care Provider Record Data (*HCPR*) (Archival Only)
- Health Care Service Record – Institutional Data (*HCSR-I*) (Archival Only)
- Health Care Service Record – Non-Institutional Data (*HCSR-NI*) (Archival Only)

Survey Data

- Beneficiary Satisfaction Survey Data (*BSURV*)

Centralized MHS System Management Data and Reference Tables

- Geographic Data (*OmniCAD*)
- Entity Identifiers/Relationships (*DMISID Index*)
- Unit Costing Data
- Other MDR Reference tables (see MDR catalog for tables in /mdr/ref/* path)
- DMIS Summary System data tables (Archival years only)

Military Medical Support Office (MMSO) Dental Data

- Active Duty Dental Plan (ADDP)
- MMSO Dental Claims (CLAIMS), data discontinued ~January 2010
- MMSO Dental Provider Records (PROVIDER), data discontinued ~January 2010

Death Data

- Casualty Data
- Master Death File Data
- Encounter Death Data

Designated Provider Data (Desprov)

- Clinical Data
- Pharmacy Data
- Provider Data

Users

The Corporate and Service Nodes presume the enterprise-level power users possess a thorough knowledge of SAS and existing MHS data sets, and are experienced healthcare analysts.

IV. System Overview and Technical Architecture

The data in this environment is a combination of SAS datasets and ASCII flat files. Most processed data reside in SAS data set form and take advantage of SAS procedure and library functions. The environment has no user interface in the traditional sense. It is intended for expert analysts only.

Software

The Corporate and Service Nodes provide access to authorized users via secure communication technologies (i.e. SSH – See Section VII, *Overview of Access Requirements*). Users do **not** have access to Graphical User Interface (GUI) functionality provided by the Common Desktop Environment (CDE). The Corporate and Service Nodes support the tools identified in Table 1.

Table 1. Corporate and Service Node Support Tools

SAS v9.12	Text Editors	Other
Base SAS SAS/STAT	PICO vi	PuTTY WinSCP

Storage - Online

Online disk storage is available to the Corporate and Service Nodes. Section X, entitled *Space Allocation and Related Issues*, contains additional information on Corporate and Service Nodes online disk storage requirements.

Storage – Near-line

In addition to online disk storage, the Corporate and Service Nodes offer near-line resources to users. Near-line resources consist of tape subsystems that allow users to conserve online disk space while retaining the ability to store and retrieve data. Additional information on near-line storage can be found in Section X, entitled *Space Allocation and Related Issues*.

Computing Resources Management (Job Priorities and Scheduling)

System administrators will monitor computing resources. Additional information on how computing resources are managed to avoid contention and maximize performance can be found in Appendix C, entitled *Load Leveler and Computing Resources Management*.

V. System Functionality

Data Refresh

The MDR data sets in this environment will be refreshed with current week, month, quarter, or yearly data immediately after MDR processing is completed. For MDR data sets that are not processed, the update will be loaded upon receipt and completion of Quality Control (QC).

Data Availability

In general, the environment contains current fiscal year (to date) plus at least two previous fiscal year data sets. Data and selected user "result sets" will be stored online or near-line.

VI. System Operations

Operational Policies/Constraints

Operational policies and constraints are outlined below:

- Updates Frequency Table. Update frequency for each data type (Table 2).
- Support. System and database administration, firewall administration, and data and systems configuration control are provided by DHSS system administration staff.
- Configuration Management (CM). Reports and "result sets" generated by users will not be placed under CM control.
- Access Restrictions. System level access will be restricted to DHSS system administration staff.
- System Security. This environment is considered an access point to the corporate MDR and as such will undergo security testing and be subject to all associated security documentation requirements.
- System Backup. Backup and recovery of output/work products are controlled by DHSS System Administration Staff.

Table 2. Update Frequency Per Data Type

Data Type	Update or Refresh Cycle
MTF Clinical System Data	
Direct Care Encounter Data (<i>SADR</i>)	Weekly – Usually every Thursday
Direct Care Encounter Data (<i>CAPER</i>)	Weekly – Usually every Monday
Direct Care Inpatient Data (<i>SIDR</i>)	Monthly – Updated on or about the 20 th day of each month
Worldwide Workload Report Data (<i>WWR</i>)	Monthly – Updated on or about the 20 th day of each month
Completion Factor Data (<i>SADR CompFac</i> ¹ and <i>SIDR Compfac</i>)	Monthly – Updated on or about the 20 th day of each month
Appointment Data (<i>APPT</i>)	Monthly – Updated on or about the 20 th day of each month
Ancillary (<i>ANCIL</i>)	Monthly – Updated on or about the 20 th day of each month
Referral	Weekly – Usually every Monday
Case Management	Weekly – Usually every Monday
Manpower, Workload, Expense Data	
MEPRS from Expense Assignment System (<i>EAS-IV</i>), includes Ancillary, Expense Detail, and Personnel	Monthly – Updated on or about the 30 th day of each month
MEPRS Executive Query System (<i>MEQS</i>)	Archival – 1996-2001 Only. Replaced by <i>EAS-IV</i> .

¹ SADR Completion Factors are only applicable for FY02 and back. FY03 and forward are "completed" based on appointment-inferred data (see SADR specification).

Data Type	Update or Refresh Cycle
Beneficiary Demographics Data	
DEERS VM6 Aggregate	Monthly – Updated on or about the 20th day of each month
DEERS VM6 Ben	Monthly – Updated on or about the 20th day of each month
DEERS VM6 ENR	Monthly – Updated on or about the 20th day of each month
DEERS VM6 LENR	Monthly – Updated on or about the 20th day of each month. Replaced by LELG.
DEERS Longitudinal VM6 (LVM6)	Monthly – Updated on or about the 20th day of each month
DEERS Special HCDP	Monthly – Updated on or about the 20th day of each month
DEERS Medicare	Monthly – Updated on or about the 20th day of each month
Reservist	Monthly – Updated on or about the 10 th day of the month
MCFAS	Annually – Updated on or about October 30 th each year
Point-in-time Extract Data (<i>PITE</i>)	Archival Only. Replaced by VM6.
Population Summaries (<i>PITE-AGG</i>)	Archival Only. Replaced by VM6.
Enrollment Data (<i>Tricare Enrollment File</i>)	Archival Only. Replaced by VM6.
Enrollment Summaries (<i>Longitudinal Enrollment File</i>)	Archival Only. Replaced by VM6.
DEERS VM4 Aggregate	Archival Only. Replaced by VM6.
DEERS VM4 Ben	Archival Only. Replaced by VM6.
DEERS VM4 ENR	Archival Only. Replaced by VM6.
DEERS VM4 LENR	Archival Only. Replaced by VM6.
DEERS Longitudinal VM4 (LVM4)	Archival Only. Replaced by VM6.
Non-Availability Statement (<i>NAS</i>) Aggregate & Beneficiary	Archival – 1994-2001 Only
Centralized Pharmacy Data	
Pharmacy Data Transaction Service (<i>PDTS</i>)	Weekly
National Mail Order Pharmacy data (<i>NMOP</i>)	Archival – 1998-2002 Only
Purchased Care Data	
Tricare Encounter Data – Institutional Data (TED-I)	Monthly – Updated on or about the 15 th day of each month
Tricare Encounter Data – Provider Data (TED-PR)	Monthly – Updated on or about the 25 th day of each month
Tricare Encounter Data – NonInstitutional Data (TED-NI)	Monthly – Updated on or about the 10 th day of each month
Health Care Provider Record Data (<i>HCPR</i>)	Archival Only. Replaced by TED-PR.
Health Care Service Record– Institutional Data (<i>HCSR-I</i>)	Archival Only. Replaced by TED-I.
Health Care Service Record– Non-Institutional Data (<i>HCSR-NI</i>)	Archival Only. Replaced by TED-NI.
Survey Data	
Beneficiary Satisfaction Survey Data (BSURV)	Archival Only. No longer updated. Last posting was 2002.
Centralized MHS System Management Data and Reference Tables	
Geographic Data (<i>OmniCAD</i>)	Monthly – Update on or about the 5 th day of each month

Data Type	Update or Refresh Cycle
Entity Identifiers/Relationships (<i>DMIS ID Index</i>)	Monthly – Updated on or about the 5 th day of each month
Unit Costing Data	Annually
Other MDR Reference tables (see MDR catalog for tables in /mdr/ref/* path)	
DMIS Summary System data tables	Archival years only
Military Medical Support Office (MMSO) Dental Data	
Active Duty Data Plan (ADDP) Claims	Monthly – Updated on or about the 25 th of each month. FY09 and forward only.
Active Duty Data Plan (ADDP) Provider Records	Monthly – Updated on or about the 25 th of each month. FY09 and forward only.
MMSO Dental Claims (CLAIMS)	Replaced by ADDP. Data through Feb 2010.
MMSO Dental Provider Records (PROVIDER)	Replaced by ADDP. Data through Feb 2010
Death Data	
Casualty Data	Monthly – Updated on or about the 15 th day of each month
Encounter Death File	Monthly – Updated on or about the 15 th day of each month
Master Death File	Monthly – Updated on or about the 15 th day of each month
Designated Provider Data	
Clinical Designated Provider	Updated Monthly – Updated on or about the 10 th of each month
Pharmacy Designated Provider	Updated Monthly – Updated on or about the 10 th of each month
Designated Provider Master Provider File	Updated Monthly – Updated on or about the 10 th of each month

Data Organization and File Naming Conventions

The MDR data sets are arrayed in a hierarchical structure using standard naming conventions. For detailed information, see Appendix B, entitled *MDR File Naming Conventions for the Corporate and Service Nodes*.

VII. Overview of Access Requirements

1. Completion of Corporate and Service Nodes Access and Security Requirements as detailed in Appendix A, entitled *Basic User's Guide for UNIX and SAS*, Section 1.
2. Fulfillment of Workstation Requirements as explained in Appendix A, entitled *Basic User's Guide for UNIX and SAS*, Section 2.
 - A. Login account to the Corporate or Service Nodes
 - B. Virtual Private Network (VPN) and/or Secure Shell (SSH) software installed on the particular workstation

C. TCP/IP hardware and software

VIII. User Support, Training and Documentation

Environment Documentation

DHSS produced informational materials, as well as documentation provided by software vendors will be made available to users as requested.

Available Documentation:

1. Online "MAN" pages
2. Basic User's Guide for UNIX and SAS (See Appendix A)
3. File Management Conventions for the Corporate and Service Nodes (See Appendix B)
4. Load Leveler and Computing Resource Management (See Appendix C)
5. Hierarchical Storage Management (HSM) (See Appendix E)

System Training

The Basic User's Guide for UNIX and SAS and support by the Corporate and Service Nodes Administration Team are available to assist users. The DHSS program office does not provide training.

IX. System Server Administration

Configuration Management (CM)

Hardware and Software CM will be handled in accordance with the policies and procedures of the DHSS Program Office. Specifically, DHSS owned software, scripts and utilities will be maintained under CM control. Scripts, programs, reports and "result sets" created by Corporate and Service Nodes users will not be managed by CM.

Backup of Output Products

Output/work products in specifically defined user directories will be written daily to backup storage. Output/work products deleted from the Corporate and Service Nodes will be deleted from backups within thirty days. DHSS system administration staff control backup and restoration of output/work products.

Physical Environment Description – Internal

The hardware platform for the Corporate and Service Nodes consists of 2 IBM System p5 Servers running AIX 5.3. The hardware resides in the DECC OKC computing facility, located in Oklahoma City (OKC), Oklahoma, and is maintained by DHSS and DISA personnel.

X. Space Allocation and Related Issues

Node Separation and Overhead

Each node requires approximately 100 gigabytes (GB) of rotating memory (disk) for system overhead and maintenance, and at a minimum, approximately 100 GB more for temporary working space in support of executing SAS programs.

File Systems: A file system is a method of storing and organizing data files, such as SAS programs, output files, SAS datasets, and text files. It also allows for manipulation and retrieval of data within and across file systems. Every file system on both the Corporate and Service Nodes has rules that set permissions for user access.

As these file systems contain “private” rather than MDR files, the government and/or functional owner of the file system is responsible for:

- Ensuring the file system contains only data authorized by law and regulation;
- Ensuring Privacy Act and Health Insurance Portability and Accountability Act (HIPAA) laws and regulations are followed; and
- Notifying DHSS of both who is empowered to provide access authorizations for that file system, and through that agent, the list of users allowed into those project or sponsor-designated files.

DHSS is responsible for assuring that any user granted access into the nodes has:

- The mandatory minimum paperwork complete and on file with DHSS to access the OKC SP and MDR data sets (ADP-II clearance, Data User Agreement (DUA), Security Awareness Certificate, and Account Access Request Form);
- Been identified by name and project/file system on an authorization document from the file system functional owner or access authority;
- Permission into those file systems for which the file system authority has granted access and no others.

“Corporate Node” File Systems

File systems will be determined based on sponsoring organization and project designation. Permissions for access are based on the information provided in the MDR Account Access Request Form (AARF). For example, /beagov/actuary is a file system for the Office of the Actuary (OACT) under the BEA (Business and Economic Analysis) construct. Only OACT analysts with permission to the file system can access this workspace. Within the file system, the OACT analysts can set up additional directories that designate analyst, task, timeframe, data type, etc. For example, /beagov/actuary/sidr would be an area where OACT wrote and ran all SIDR related programs.

“Services Node” File Systems

Each of the three services has space allocated for the creation of file systems. Organizations within the Services can have file systems created that represent their organization. For example, the Navy has a file system called /bumed which is designated for all users with access associated with the Navy Bureau of Medicine and Surgery (BUMED). The Navy can request file systems be created under /bumed, thus limiting the access to just a subset of all BUMED

analysts. For example, /bumed/specstudy might be a file system created that only allows those users involved in the "special study" to have access to that particular area.

Privacy Act and HIPAA Information

Health Insurance Portability and Accountability Act (HIPAA) requires healthcare systems to record any use or disclosure of an individual's healthcare data.

Keeping "Logs"

In healthcare systems such as the Corporate and Service Nodes, DHSS can identify data access or disclosure to the point of knowing which Corporate or Service Node user tapped which MDR data file on a specific date. In order to fulfill the remainder of the requirement for records of access, **each Corporate or Service Node user must retain "logs" of program executions on any files containing Privacy Act data.** These "logs" can be the normal electronic logs produced by SAS and stored by the user on the SP. Upon request, these logs must be made available to DHSS, TMA Privacy Office, or DHCAPE (formerly BEA).

One example for automatically saving the SAS logs to a dedicated "log" directory includes the following SAS macro which is coded at the beginning of every SAS program:

```
%let dir1=%str(/main/secondary/task/log/);
%let pgmname=%str(xxxpgm_name);
%let date=&sysdate;
%let time=&systemtime;
%let ext1=%str(log);
%let break=%str(-);
%let final1=&dir1&pgmname&date&break&time..&ext1;
%put &final1;
proc printto log="&final1";
run; quit;
```

/main = the main directory of your dedicated workspace (e.g., /beagov)

/secondary = secondary directory, if applicable (e.g., /beagov/actuary)

/task = specific task name (e.g., /beagov/actuary/uniquuser)

/log = log directory set up for each task (e.g., /beagov/actuary/uniquuser/log)

xxx = users initials

pgm_name = program name

The field final1 is the concatenation of the directory reference on line 1, the program name, date, time, and extension all referenced in the steps.

For example, if Unique Users investigation is the task, create a directory under /beagov/actuary/ called uniquuser > /beagov/actuary/uniquuser/.

Then create /beagov/actuary/uniquuser/log which is where all the logs, every time the program is run, will be stored for future reference, if necessary.

Notes:

- 1) create "task" areas for easier reference
- 2) use program names that make sense for the task
- 3) user initials allows for identification of who ran the program

If you use the above code, you MUST use the following to submit the program:
/beagov/actuary/uniquser > sas pgm_name.sas -altlog pgm_name.log

The -altlog pgm_name.log portion of the command also puts a *.log file in the directory you submitted the program from and is where the programmer can review the results of the program. So, essentially two duplicate logs are created, one for the programmer to review, the other to be HIPAA compliant. The HIPAA compliant log never gets overwritten. The reviewer log gets overwritten every time the program is rerun.

Storing and Securing Privacy Act Data

Users are responsible for full compliance with HIPAA and the Privacy Act for data created or placed into all files systems on the Corporate or Service nodes. DHSS does not track data stored in user workspace within these file systems. Private Health Information (PHI) data created as a result of programs extracting data from the MDR datasets for download or those originating outside of the OKC SP and imported/uploaded/keyed into these file systems must be reported via e-mail to the functional proponent, Dr. Richard Guerin, Director of TRICARE Management Activity (TMA) Defense Health Cost Assessment and Program Evaluation (DHCAPE, formerly BEA), care of his point of contact, Mr. James Huber.

The e-mail should be sent to James.Huber@tma.osd.mil **before the file is downloaded or uploaded**. Multiple files can be listed in the same e-mail. The e-mail needs very minimal content to include a brief description of the file, approximate size, source, and destination file system, along with your identity and organization. This information may be used to determine if an Import or Export Transmittal form is required (e.g., large amounts of data).

Downloads of PHI data that are 10,000 rows or greater requires an [Export Transmittal](#) request. Users should not download this data themselves via WinSCP or any other FTP software.

EXAMPLE OF DOWNLOADING EMAIL:

25-March04: Downloaded Direct Care SIDR and SADR records from /xyz/abc to hard drive; ~2,500 records total, with PHI and PII data. Delivered to OTSG Decision Support Center via secure FTP (HIPAA compliant). Data deleted from hard drive after delivery. John Doe, ABC Company (TMA DHCAPE).

EXAMPLE OF UPLOADING EMAIL:

25-March-04: Uploaded DMDC-provided file containing 2,500 activated guard/reserve records with SSNs and minimal activation information, saved into the corporate node's "ABC Company" file system. John Doe, ABC Company (TMA DHCAPE).

The requirement to log the existence, distribution, and destruction of files containing PHI data created on the Corporate or Service node applies to files created from the MDR as well as those placed there by users.

Migration to Near-line

Near-line storage employs an approach called Hierarchical Storage Management (HSM). Files are staged to tape storage, but remain visible to and manageable by end users. During the initial file system setup the authority works with the system administrator to determine automatic

migration to near-line storage. The file system authority may select a migration rule for implementation by DHSS, within the constraint that there must be a single rule for all files in a file system (i.e., migrate all files within file system 'x' if they have not been used in 'y' days). Additional information on the use of HSM for near-line storage of files can be found in Appendix E, entitled *Hierarchical Storage Management (HSM)*.

Appendix A. Basic User's Guide for UNIX and SAS

Basic User's Guide for UNIX and SAS

Table of Contents

[Section A-1. Corporate and Service Nodes Access and Security Requirements](#)

[Section A-2. Workstation Requirements](#)

Access through the Firewall
Encryption Software Requirements

[Section A-3. Connecting to the Corporate and Service Nodes](#)

Juniper OOB SSL VPN
PuTTY for Secure Shell (SSH) Login

[Section A-4. Transferring Files to/from the Corporate and Service Nodes](#)

WinSCP for Secure File Transfer

[Section A-5. Submitting SAS Jobs in the Corporate and Service Nodes](#)

Running a SAS Job
Using Environment Variables
Checking Job Status
Canceling a Submitted Job

[Section A-6. Moving Files to the OKC Corporate and Service Nodes from External Systems](#)

[Section A-7. Copying Files from the OKC Corporate and Service Nodes to External Media](#)

[Section A-8. Using PKZIP](#)

[Section A-9. Metadata for MDR Files](#)

What is Metadata?
Viewing Metadata for MDR Files

[Section A-10. The PICO Editor](#)

[Section A-11. Basic VI Editor – A Beginner's Guide to vi and ex](#)

[Section A-12. Changing Your OKC SP Password](#)

[Section A-13. Commonly Used UNIX Commands](#)

Command Reference Table

[Section A-14. UNIX File Naming Conventions](#)

Absolute Naming
Relative Naming
Short-cuts for File Naming
File Naming Limitations
File Name Extensions

[Section A-15. The UNIX Directory Tree](#)

Getting Around Directories

[Section A-16. Resource Considerations \(Getting More Workspace\)](#)

[Attachment A-1 Import Transmittal Form](#)

[Attachment A-2 Export Transmittal Form](#)

Section A-1. Corporate and Service Nodes Access and Security Requirements

The Corporate and Service Nodes contain “private” rather than MDR files, therefore, the government/functional owner of the file system is responsible for notifying DHSS of both who is empowered to provide access authorizations for that file system and through that agent, the list of users allowed into those project or sponsor-designated files.

Once a user has authorization from the File System Functional Owner or Access Authority, they must complete the mandatory paperwork and ensure that this paperwork is on file with DHSS in order to gain access to MDR data sets. See Appendix D, entitled *Corporate and Service Nodes Access and Security Requirements*, for details on fulfilling these requirements.

Section A-2. Workstation Requirements

DISA secures the Corporate and Service Nodes and MDR environment through the use of firewalls, VPNs, and encryption software.

Access through the Firewall

All Corporate and Service Node users are required to connect securely through the firewall using a Juniper SSL VPN solution called the Out-of-Band (OOB) SSL VPN. Access to the OOB SSL VPN is managed by DISA. DISA authorizes access to specific servers based on an approved DISA DD2875 Form. See Appendix D, entitled *Corporate and Service Nodes Access and Security Requirements* for details.

Encryption Software Requirements

The Corporate and Service Nodes accept encrypted connections only. Once authorized through the firewall using the OOB SSL VPN solution, all users must connect to the Corporate and Service Nodes using SSH connection software. See Table 3 for information on recommended login and file transfer utility software.

Table 3. Login and File Transfer Utility Software²

Recommended SSH Software for:	
Login	PuTTY
File Transfer	WinSCP

Detailed instructions on download and use of SSH software such as PuTTY and WinSCP may be found in Section 3, entitled *Connecting to the Corporate and Service Nodes* and Section 4, entitled *Transferring files to/from the Corporate and Service Nodes*.

Users behind firewalls using SSH: The Corporate and Service Nodes utilizes a Secure Shell (SSH) connection that communicates over “common” TCP Ports. These ports must be granted access through your firewall. **Contact your local Network Administrator to ensure that TCP Port 22 is open.**

² Please note that there are numerous Secure Login and File Transfer clients available. This document illustrates connectivity using PuTTY for Secure Login and WinSCP for Secure File Transfer.

Section A-3. Connecting to the Corporate and Service Nodes

Most users are required to use the Out-of-Band (OOB) Secured Socket Layer (SSL) Virtual Private Network (VPN) to authenticate through the OKC Firewall. At this time, users behind a *.mil network can access the Corporate and/or Service nodes using the OOB or a non-OOB solution. Non *.mil (e.g., *.com) do not yet have a non-OOB access to the nodes; this is being investigated. See PuTTY for Secure Shell (SSH) Login, page 24, for the setup and IP address for the non-OOB solution.

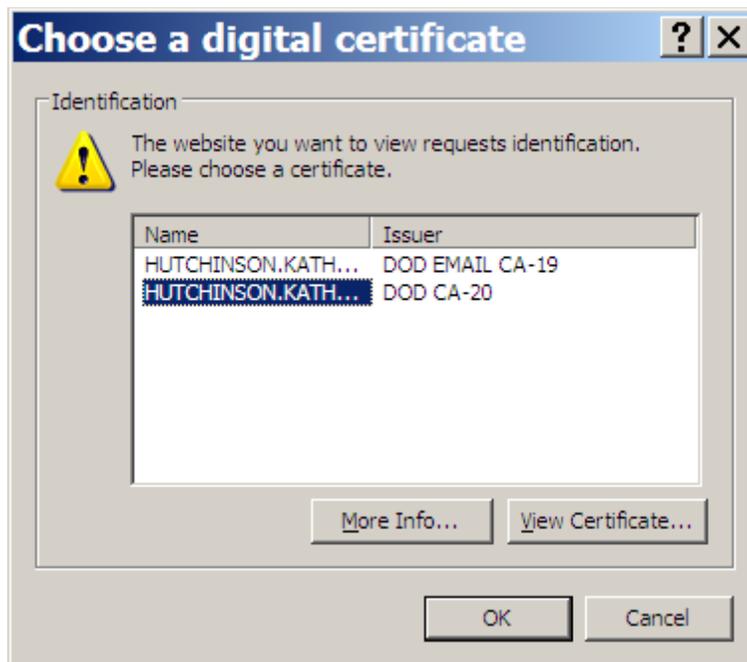
Once authenticated, users are required to use Secure Shell (SSH) software to connect to the server. See below for detailed instructions on accessing and initializing the OOB SSL VPN webpage and invoking PuTTY SSH software.

Juniper OOB SSL VPN

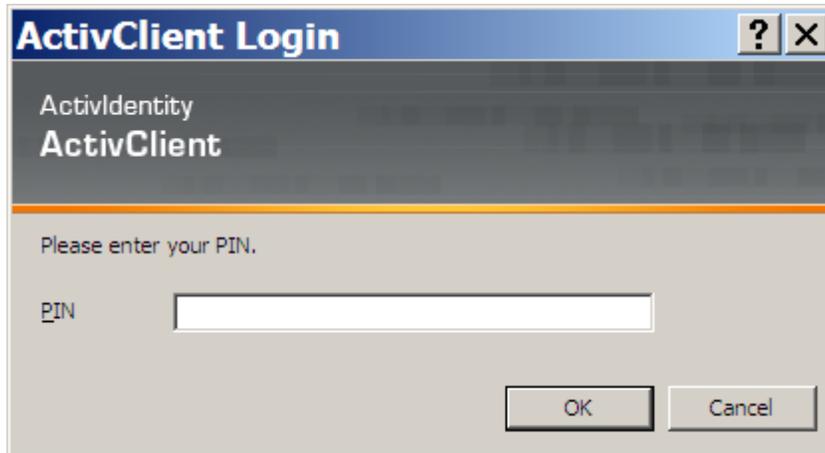
By using these instructions you will be able to create a VPN between your workstation and DHSS Systems located in DECC OKC. Once the VPN is established, it locks out all other ports (no internet access, no printing, no email, etc.)

Juniper OOB SSL VPN Instructions

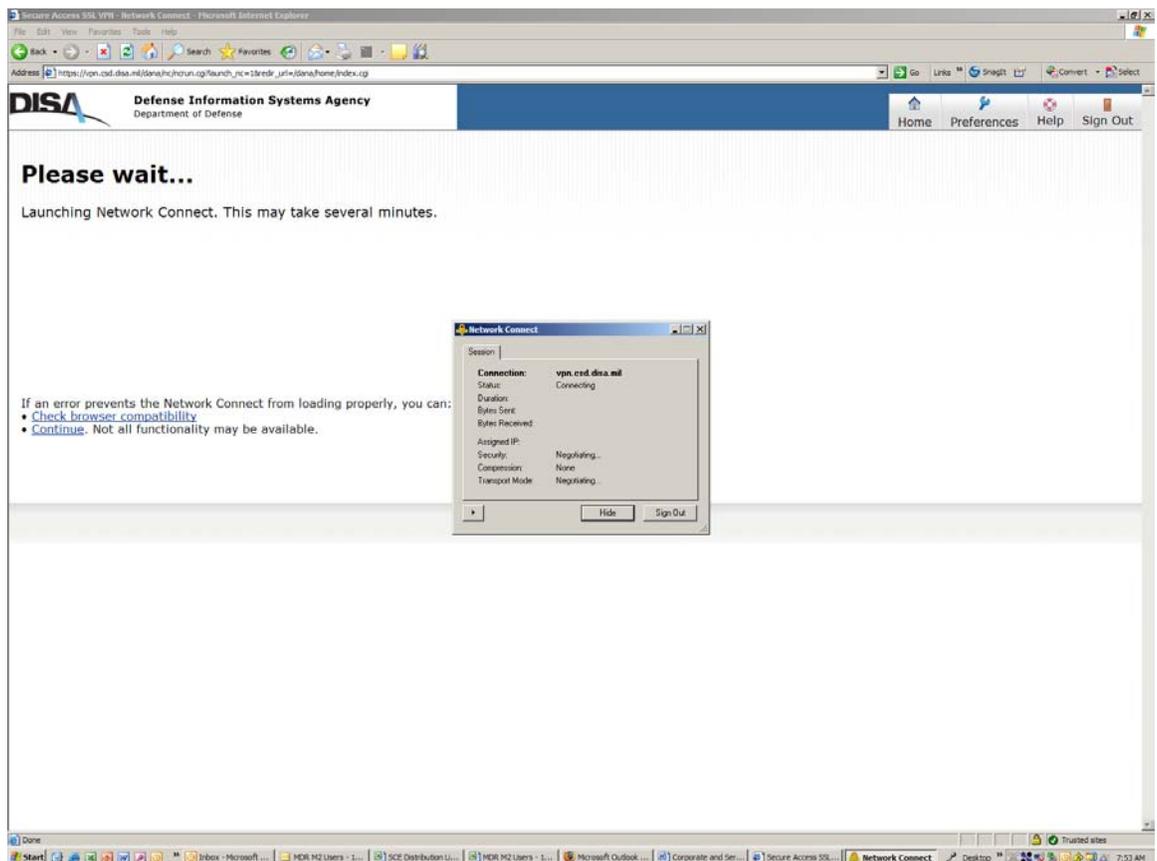
1. Insert your Common Access Card (CAC) in the CAC Reader.
2. Access the Juniper SSL via <https://vpn.csd.disa.mil/oob>
 - The first time you access this URL it will ask to install a JAVA applet which requires administrative privileges to your machine.
 - Next it will verify the certificate on your CAC. Choose the non-email name (e.g., from below, choose the line with Issuer DOD CA-20, not DOD EMAIL CA-19). Click OK.



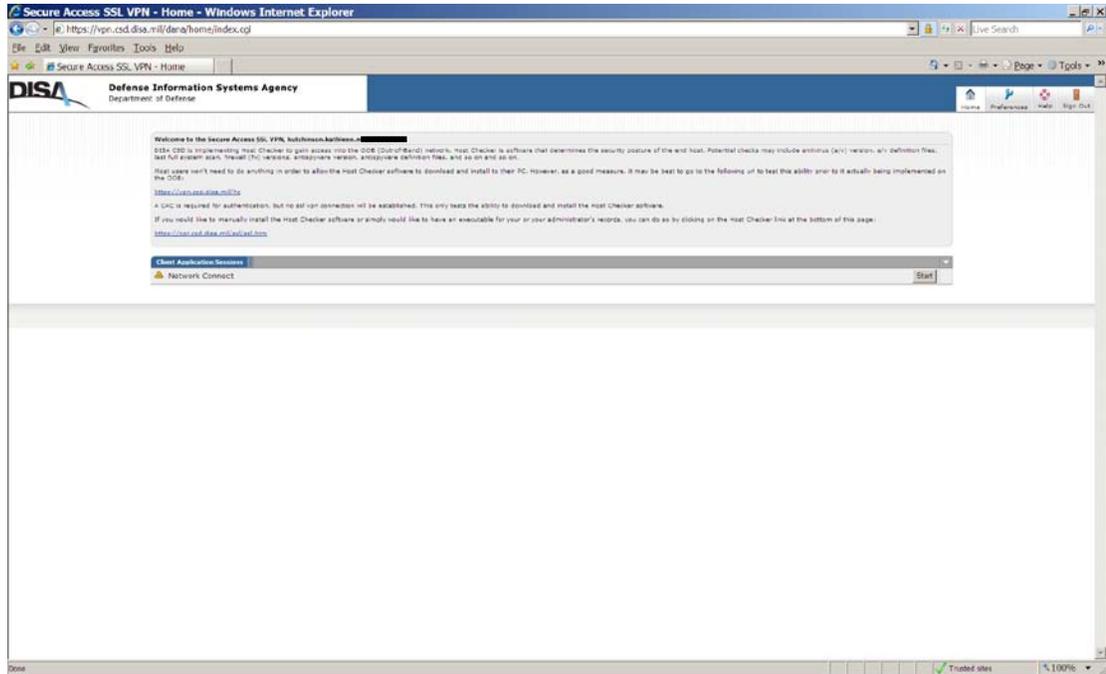
- ☑ Enter your PIN for your CAC.



- ☑ The VPN will negotiate your information to ensure it has permission to connect.



- ☑ After a few moments you should see a screen similar to the following.

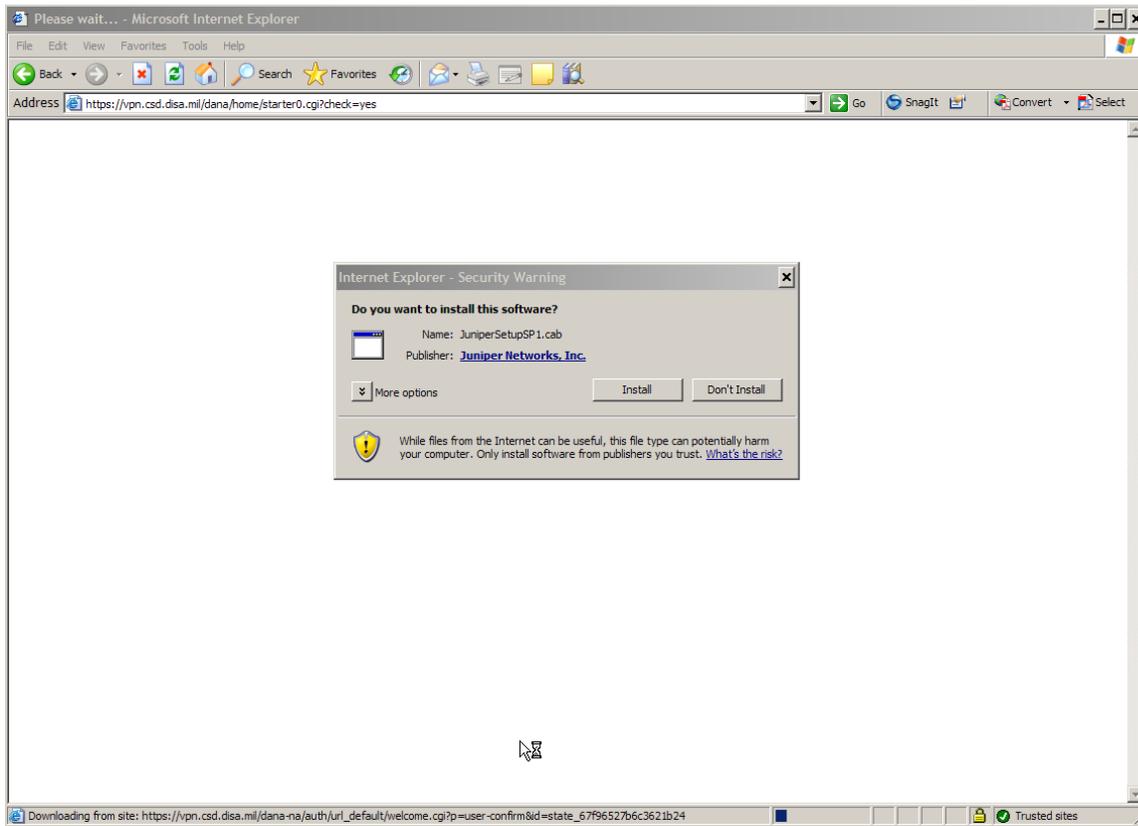


- ☑ A lock with alternating green circles will be present during your secure session in your tray. It is highlighted by the red circle below. Sometimes the web page may indicate an error, but as long as the lock with green lights is present the OOB is still connected for a secure session.

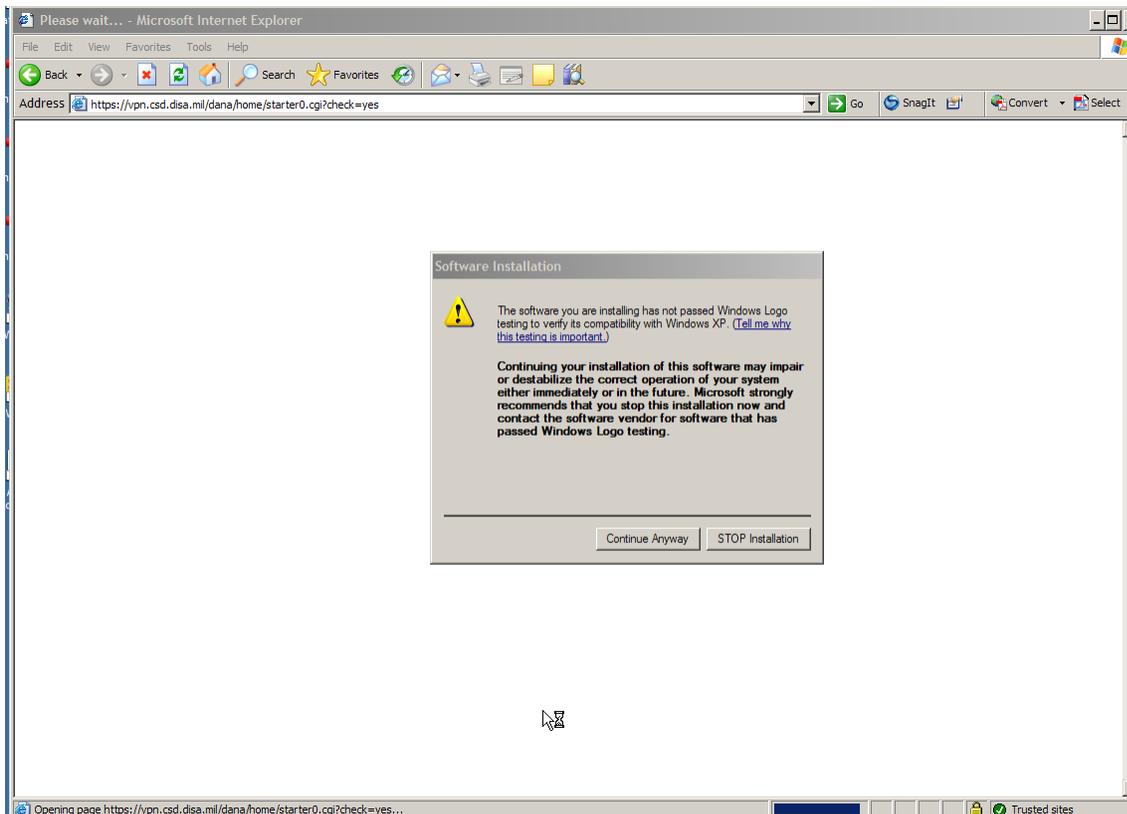
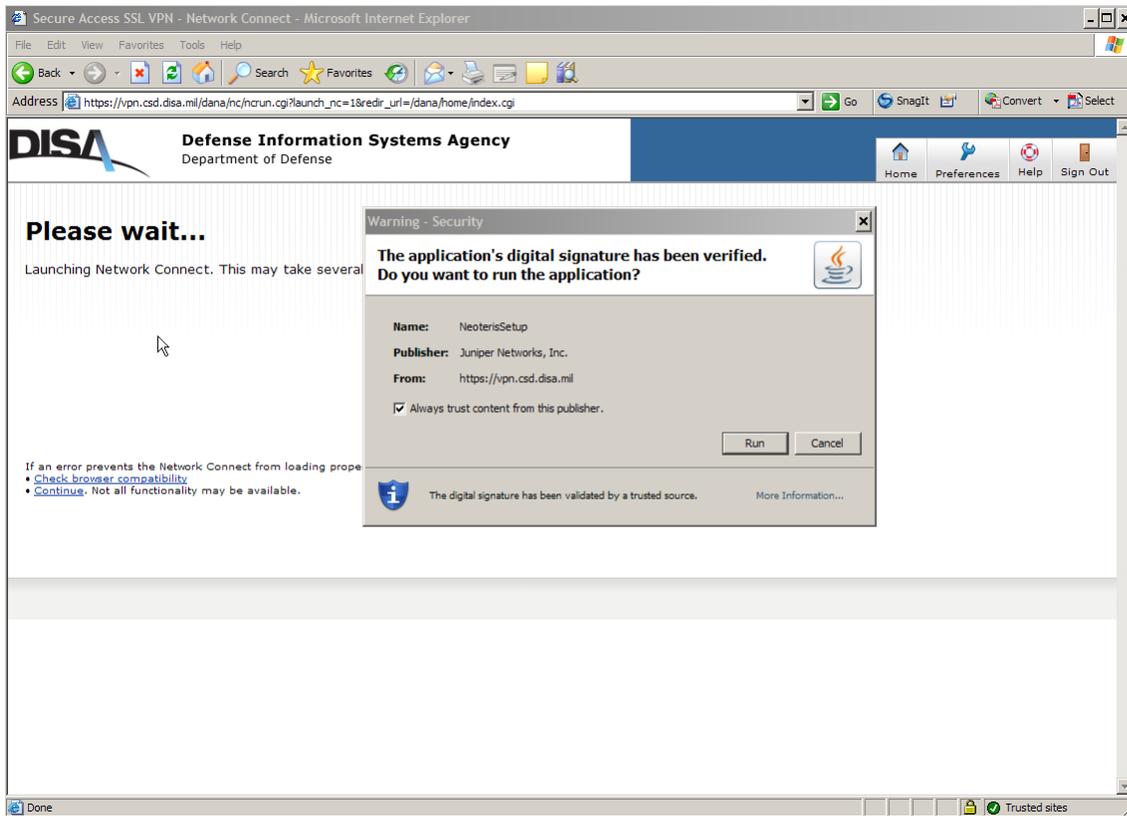


OKC DISA Juniper Tool Updates

OKC DISA will attempt to push out automatic updates to the Juniper tool on a periodic basis. Users must have administrative permission for the tool to be installed automatically as designed by OKC DISA. The following two screen shots are potential updates that might be encountered on a periodic basis using ActiveX when you attempt to log onto the OOB. If the update fails to install, work with your local help desk to have them install the tool.



The second tool pushed by OKC DISA has not been consistent for all users. Microsoft suggests rejecting the installation, but you will not gain access via the OOB unless it is installed if prompted. The install radial button needs to be selected between 6 to 8 times for the tool to install.



Once again, if the automated installation fails, the administrative rights are needed to use the Microsoft Control Panel to uninstall Juniper 6.0 and install Juniper 6.3. The tool can be downloaded from the following URL.

Go to <https://opr.csd.disa.mil/ssl/ssl.htm>

Download and install the 'Juniper Installer Service.'

Try to reconnect to the VPN

PutTY for Secure Shell (SSH) Login

1. Once the account is approved and permissions set, users will be provided information on their Corporate or Service Node user ID, work space, and how to obtain their temporary password for accessing the system.

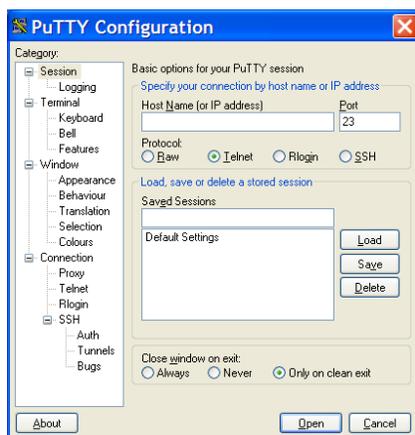
As a first step, users will be required to change their temporary password to a permanent, 15-character password (see Section A-12) by signing onto the password server. The steps below include the password server IP address. It is recommended that users have their new password ready as the system will close if there is a delay entering the new password.

Downloading PuTTY

2. Go to the following website to download PuTTY:
<http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html>
3. Scroll down to the section titled, 'The latest release version' and find your operating system. Click on 'putty.exe' to download.
4. Save the executable to your workstation.
 - PuTTY is a little larger than 350 KB in size.
 - This is where you will invoke PuTTY in the future.
5. Once the download has completed successfully, double click the icon for "putty.exe".

Initializing PuTTY

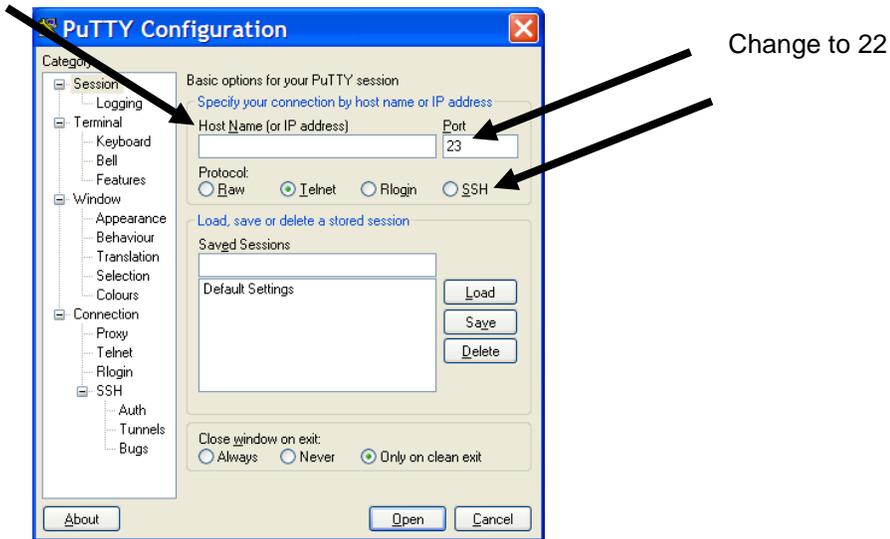
You will be presented with a PuTTY Configuration screen.



- Enter the **IP address** of your Corporate and/or Service Node under *Host Name (or IP address)* and specify the **Port** number to be 22:

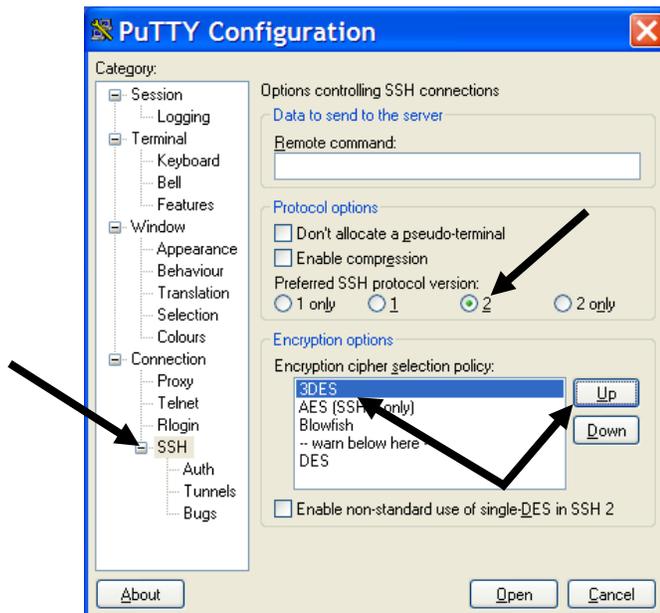
Corporate Node: 2.15.123.16 (address to use with OOB)
 Services Node: 2.15.123.17 (address to use with OOB)
 Password Server: 2.15.123.5 (address to use with OOB)

Corporate Node: 152.229.239.34 (non-OOB address, *.mil only)
 Services Node: 152.229.239.35 (non-OOB address, *.mil only)
 Password Server: 152.229.239.47 (non-OOB address, *.mil only)

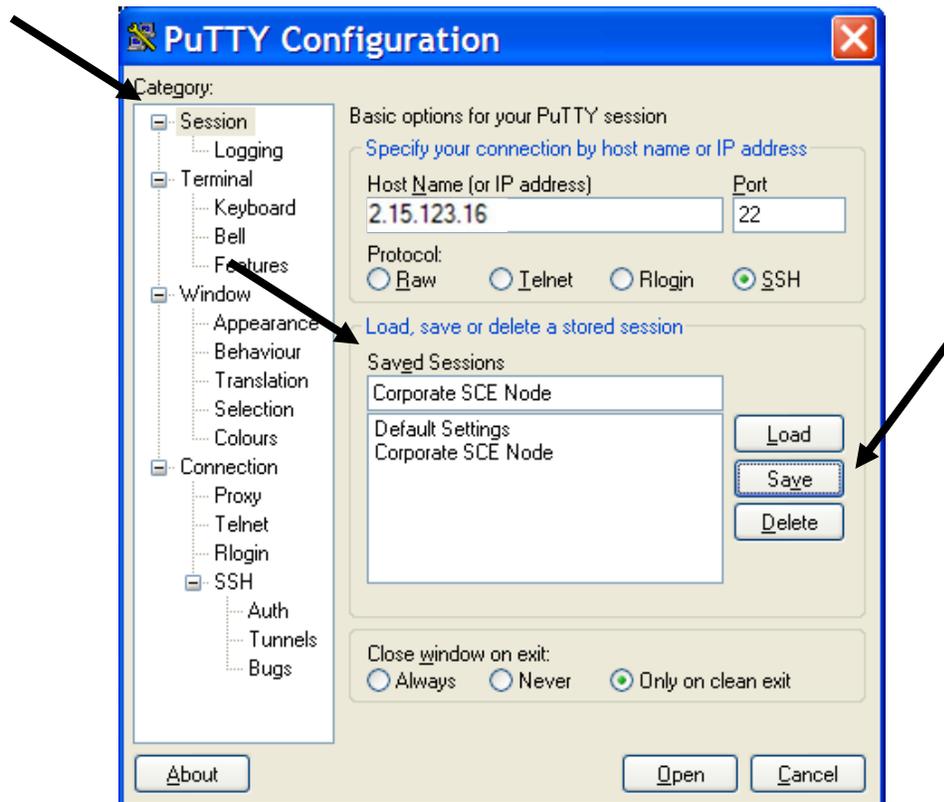


- Click on **SSH** under *Protocol*.
- On the left-hand side of the window, under *Category, Connection*, click on **SSH**. Ensure that you have:

Preferred SSH protocol version = **2**
 Preferred encryption algorithm = **3DES** (Select 3DES and select Up button until 3DES is first as depicted below)



9. Click on **Session** under *Category*. Enter a 'nickname' in the *Save Sessions* field, and click on **Save**. Doing this will prevent you from having to enter this information each time you log on.



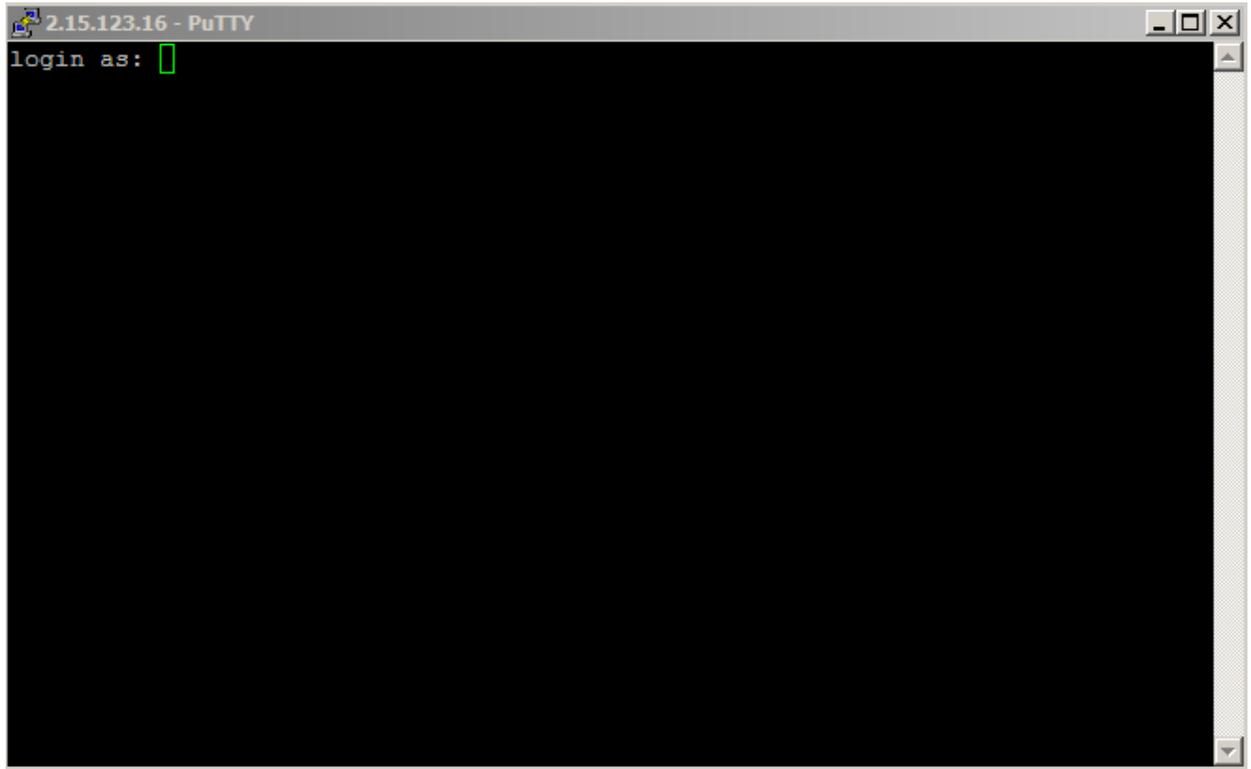
10. When you are ready to connect, double-click the *Saved Sessions* name OR click the *Saved Sessions* name, **Load**, and then **Open**.
11. You will be presented with the following window. Click **Yes** to accept the key from the SSH server running on the Corporate and/or Service Node.

Note: This screen will only appear the first time you log on to the node and accept the server's host key.

Note: Please install recommended software upgrade over existing PuTTY executable. This will ensure the proper version is installed.



12. Finally, a login prompt will appear. Type your **Corporate or Service Node User ID** and hit enter. Type your **Corporate or Service Node password** and hit enter. When ready, simply type **exit** to exit the system and close your PuTTY session.



After closing the PuTTY session, double click or right click the Network Connect icon in the bottom right (lock with blinking green lights) and click Sign Out. It may take a few seconds for the disconnect to complete. Then click Sign Out (upper right) in the OOB session.

Section A-4. Transferring Files to/from the Corporate/Service Nodes

WinSCP for Secure File Transfer

WinSCP is the recommended client for securely transferring files between the Corporate and/or Service Nodes and your PC. WinSCP is a windows-based program similar to FTP.

Downloading WinSCP

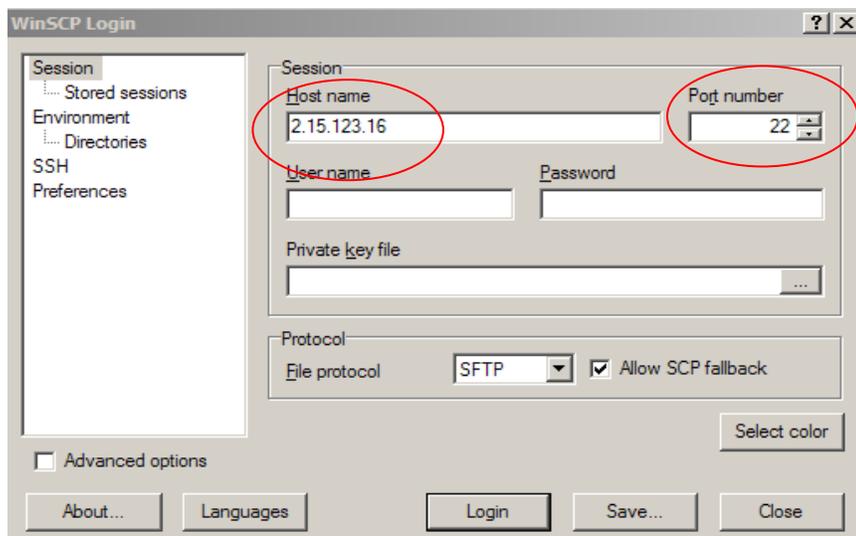
1. Go to the following website to download WinSCP (<http://sourceforge.net/projects/winscp/>)
2. From the green *Download Now!* button, click on *View all files*.
3. Under the All Files section expand the latest, non-beta, version of WinSCP. Once expanded, click on the executable (winscpxxx.exe, where “xxx” is the version number).
4. Save the executable to your workstation.
 - WinSCP Application is approximately 1.24 MB in size.
 - This is where you will invoke WinSCP in the future
5. Once the download has completed successfully, double click the icon for “WinSCPxxx.exe” where xxx is the most recent version available.

Initializing WinSCP

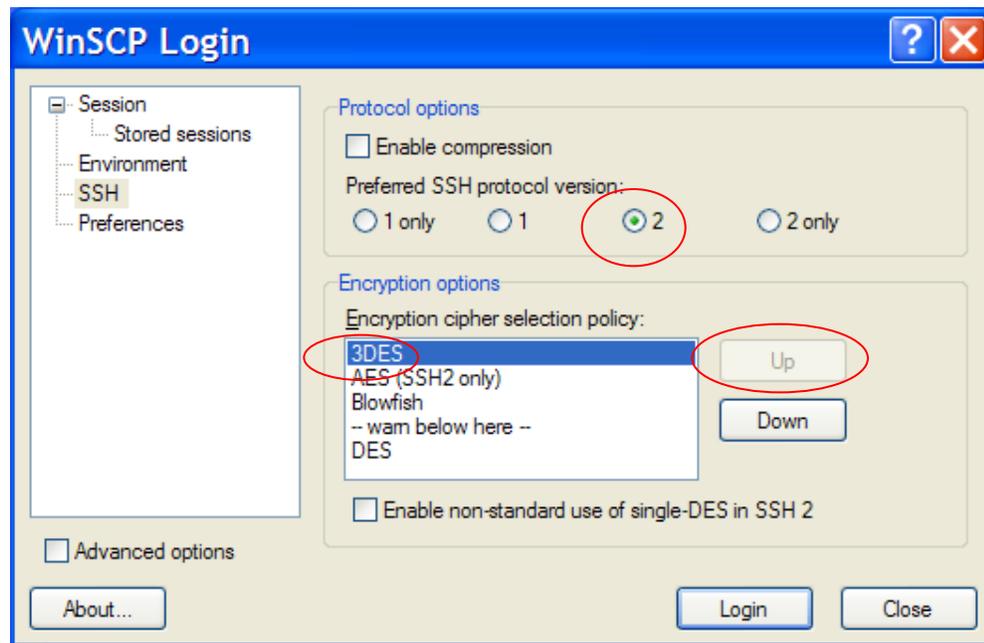
You will be presented with a WinSCP Login screen.

6. Under *Session, Stored sessions*, click the *New* button on the right-hand side of the screen.
7. Under *Host name*, enter the **IP address** of the CORPORATE OR SERVICE Node you are connecting to and **Port** number to be 22:

Corporate Node:	2.15.123.16 (address to use with OOB)
Service Node:	2.15.123.17 (address to use with OOB)
Corporate Node:	152.229.239.34 (non-OOB address, *.mil only)
Service Node:	152.229.239.35 (non-OOB address, *.mil only)
8. Under *User Name*, enter your **CORPORATE OR SERVICE User ID**.
 - DO NOT enter your password at this time.
 - Select **SFTP** radial button within the *Protocol* Dialogue Box

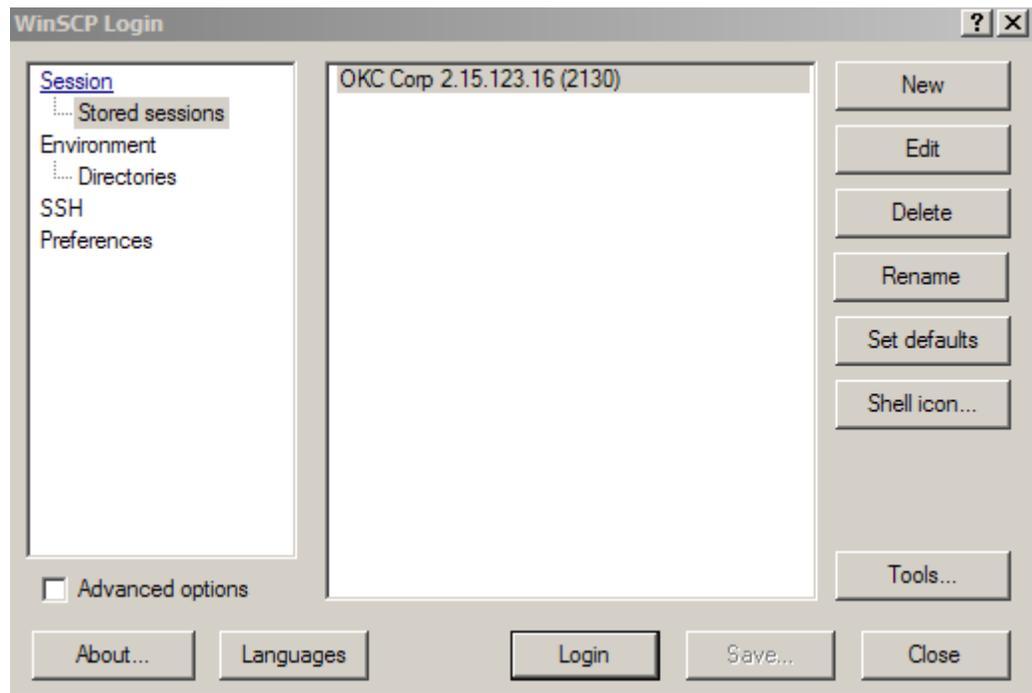


- On the left-hand side of the window, click on **SSH**. Ensure that you have:
Preferred SSH protocol version = **2**
Encryption cipher selection policy = **3DES** (Select 3DES and click the **Up** button until 3DES is first as depicted below)



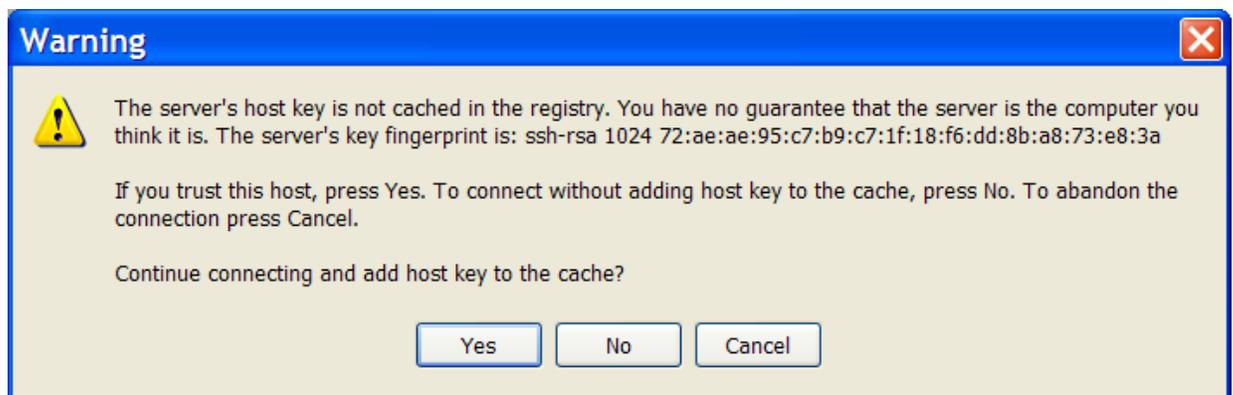
- Click **Save** to store this information in WinSCP. A "Save session as" window will appear prompting you to save the information. Enter your desired profile name and click **OK**.

11. When you are ready to connect, double-click the *Stored Sessions* name OR click the *Stored Sessions* name, **Load**, then **Login**.



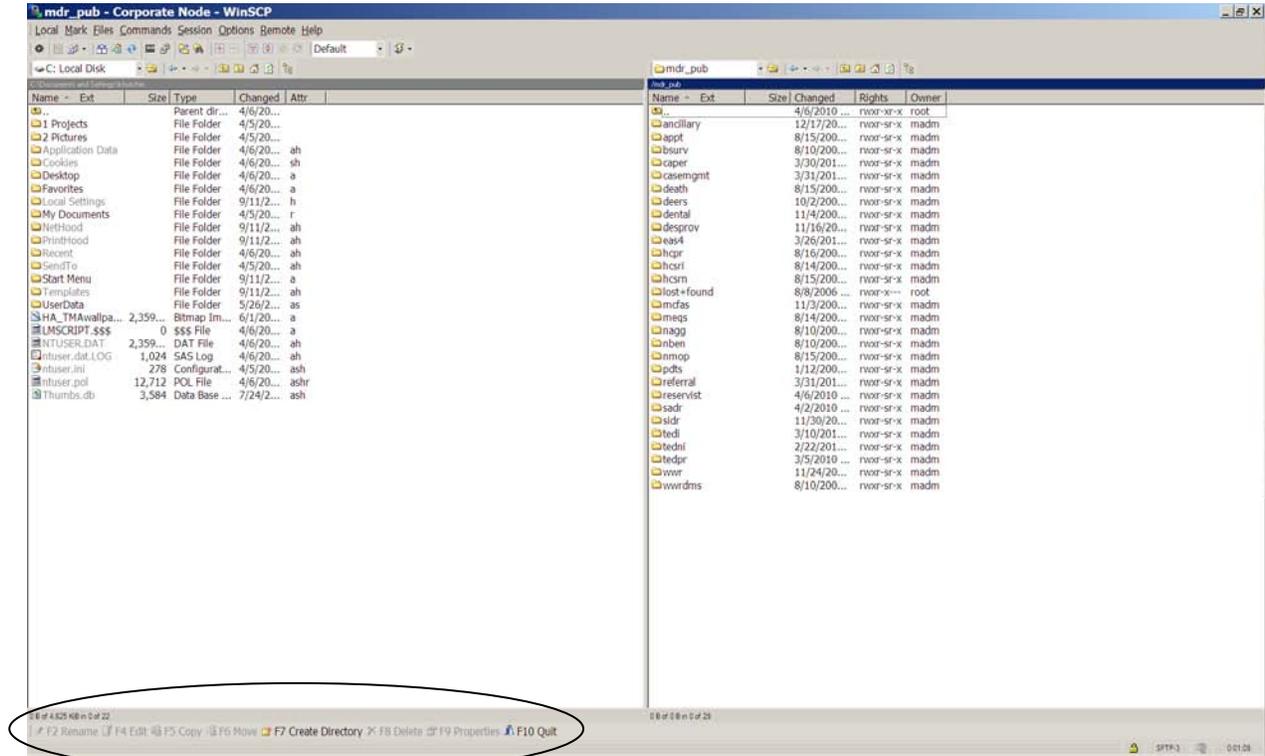
12. You will be presented with the following window. Click *OK* to accept the key from the SSH server running on the Corporate or Service Node.

Note: This screen will only appear the first time you log on to the node using WinSCP and accept the server's host key.



13. When prompted, enter your **Corporate or Service Node Password**.

- Upon successful connection, a similar WinSCP screen will appear. The WinSCP environment functions are similar to Windows Explorer. See the menu bar at the bottom of the window for direction on how to rename, copy, move, or delete files and disconnect from WinSCP.



Section A-5. Submitting SAS Jobs in the Corporate or Service Nodes

Running a SAS Job

SAS jobs run in the background within the Corporate or Service Nodes preventing running jobs from failing if the VPN or SSH session times out. You may create or edit SAS programs within the Corporate or Service Nodes using the PICO or vi editor. If you prefer to work on your PC, you may edit your programs in Windows and then use WinSCP to copy them to the node.

Due to the high usage of the MDR, to include the Corporate and Service nodes SAS Computing Environments, there is a limit of 3 programs /submissions per user at any one time. If more than 3 are submitted, the most recent submission may be cancelled without warning.

Important: In order for programs to run, they MUST be named with a .sas extension.

To submit a SAS job:

1. Log on to the node using PuTTY and change to the directory where the SAS program is located in your file system space.

Example:

```
/trailhome/userid> cd /hpa2/
```

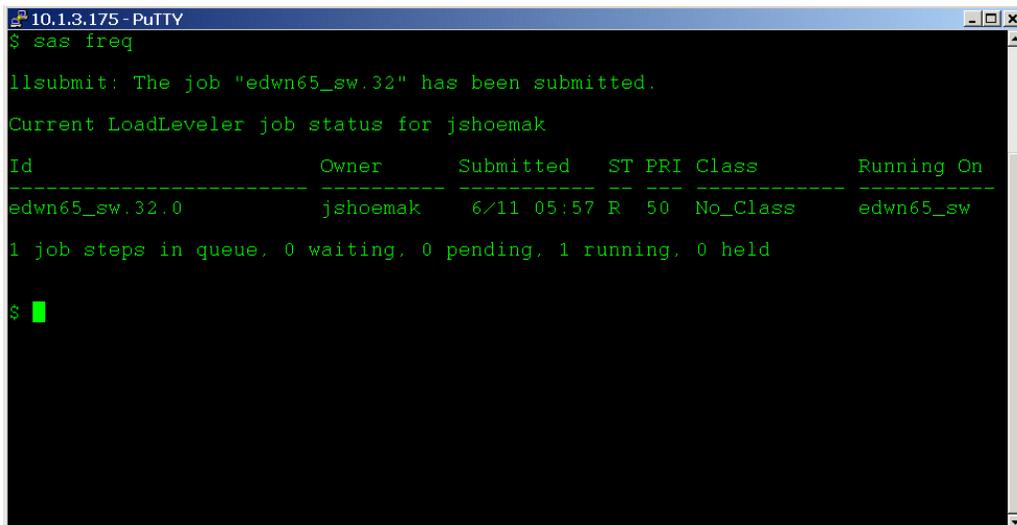
Note: Do not store code or data in your user directory, specifically /trailhome/userid.

2. Submit the program by typing:

```
/hpa2> sas <program_name.sas>
```

Remember, if the macro described in Keeping Logs is used (page 15), you must use the syntax provided in that section to submit your programs.

```
sas <program_name.sas> -altlog <program_name.log>
```



```
10.1.3.175 - PuTTY
$ sas freq

llsubmit: The job "edwn65_sw.32" has been submitted.

Current LoadLeveler job status for jshoemak

Id              Owner      Submitted   ST PRI Class      Running On
-----
edwn65_sw.32.0  jshoemak   6/11 05:57 R  50  No_Class    edwn65_sw

1 job steps in queue, 0 waiting, 0 pending, 1 running, 0 held

$ █
```

Your program will be submitted through Load Leveler as a background process and run immediately. Forty-eight jobs are able to run on the Corporate or Service Node in SASwork and eight/four jobs on the Corporate/Service Node in BigSASwork concurrently. Any jobs after that enter a queue to be executed sequentially.

Using Environment Variables

Because Load Leveler is a batch scheduling application, any environment variable defined in the shell when Load Leveler is invoked will not be passed to the SAS program. In order to use environment variables in your SAS program, they must be defined by the SET option when SAS is invoked. This can be done using the following:

```
sas <program_name> -SET <variable_name> <value>
```

Using SAS 9 and SAS Temporary Workspace

SAS 9 has been loaded for both Corporate and Service Node jobs. SAS temporary workspace environments exist for the Corporate and Service Node jobs, separately. Please use the guidelines below and commands for using the appropriate SAS workspace and submitting SAS jobs.

Table 4. Temporary Workspace Definitions

SAS Temp. Workspace	SERVICE NODE Combined Workspace Requirements of:	CORPORATE NODE Combined Workspace Requirements of:
Small (Normal)	Less than 10 GB	Less than 30 GB
Large (Big)	Greater than 10 GB	Greater than 30 GB

Commands for submitting SAS Version 9 jobs on the Nodes

- To start a job requiring less than 10GB for the Service Node or 30GB for the Corporate Node of combined SAS workspace (runs in the normal workspace), the command is **sas *jobname***
- To start a job requiring greater than 10GB for the Service Node or 30GB for the Corporate Node of combined SAS workspace, the command is **sasbig *jobname***
- To determine what jobs are running in the SAS Temporary Workspaces simply type **'llq'** at the command prompt and look under "Class" to determine the jobs running or queued to run in the Normal, and Big SAS Temporary Workspaces.

Checking Job Status

To find the current status of running jobs, type llq at the command prompt.

```

10.1.3.175 - PuTTY
jshoemak@edwn65:~$ llq
-----
Job ID      Owner      Submitted   ST PRI Class      Running On
-----
edwn65_sw 32.0      jshoemak   6/11 05:57 R  50 No_Class  edwn65_sw

1 job steps in queue, 0 waiting, 0 pending, 1 running, 0 held
jshoemak@edwn65:~$

```

All submitted jobs have completed when the output reads:

llq: There is currently no job status to report.

Check the .log files for results.

Canceling a submitted Job

To cancel a submitted job, use the 'sasstop' command, which is an interactive application. It will list all the jobs you have currently running in the system and ask you which job you want to delete. If no jobs are running, it will inform you of that fact and exit.

To invoke 'sasstop' in the Corporate or Service Nodes, type sasstop at the command prompt.

Note: 'sasstop' will only allow a user to cancel their own submitted jobs. Jobs submitted by other users are not shown in the list nor are able to be cancelled by non-owning user accounts.

Note: Sometimes SAS jobs which terminate abnormally leave residual data within the temporary SAS work space. This data will be removed by the system administrator on a routine basis.

Remember, do not store programs, scripts, data, formats, etc. under your user home directory /trailhome/userid/. There is very limited space available for the home directories. If this space becomes full, all users will be locked out of both the Corporate and Service Nodes. If the system administration staff sees files in the home directories other than those placed there by the staff, they will be removed after due diligence.

Section A-6. Moving Files to the Corporate/Service Nodes from External Systems

Corporate or Service Node users may periodically require files be made available on the node(s) that only exist on external systems and for which using WinSCP is not an option. Following are instructions for having a file(s) moved to the Corporate or Service Nodes.

1. Ship Tape(s) to DHSS Corporate or Service Node Administration Staff

Coordinate with the external system source to have the file(s) written to DVD, CD-ROM, USB disk drive or one of these tape formats: DLT, IBM 3480, IBM 3490, or LTO. Ship the media to the following address:

**DHSS Corporate or Service Node Administration Staff
c/o ABSi
5111 Leesburg Pike, Suite 706
Falls Church, VA 22041**

If you need additional information, please contact the following personnel:

- matthew.kapusta@absicorp.com
- Kathleen.Hutchinson.ctr@tma.osd.mil
- Martin.Shepherd.ctr@tma.osd.mil
- Fauzia.Jones.ctr@tma.osd.mil
- corinna.barnes@absicorp.com
- beth.pelletier@absicorp.com

2. Complete an *Import Transmittal Form*

Complete an Import Transmittal form by supplying the following information. The Import Transmittal form may be found in Appendix A, entitled *Basic User's Guide for UNIX and SAS*, Attachment A-1.

Section 1 - Requestor Information

- Requestor Name & Company - The Corporate or Service Node user requesting the data and their company name.
- Requestor Information - The phone number and e-mail address of the requestor.
- Return the tape(s) - Does the tape(s) need to be returned to the source? Check the appropriate box. If the tape(s) does need to be returned, provide the shipping information such as POC, address and phone number.

Section 2 - Media Characteristics

- Media Type - Indicate the media format to be read (CDROM, DLT, IBM 3480, IBM 3490, or LTO).
- Total Number of CDs/Tapes – This is the total number of CDROMs/Tapes to be read in.
- For CD-ROM, DVD, and USB Drives, list the file names to be read in to the Corporate or Service Node.
- For Tapes, indicate the following:
 - Application used to create the tape – i.e. tar, ReelExchange, NT Backup, etc.
 - Data Format of the Tape(s) - ASCII or EBCDIC
 - Label Type – ANSI, EBCDIC, or UNLABELED
 - In this order, provide the file name, record format (fixed block=fb, variable block=vb), block size, line count, record length, and logical volume serial number.

For example, if you have one file named myfile, which is in fixed block format, contains a line count of 54,980, block size of 32,760, record length = 196, and has a logical volume serial number = 770076, the Tape Transmittal would display the information as:

File name : record format : block size : line count : record length : logical volume serial number	myfile : fb : 32760 : 54980 : 196 : 770076
--	--

Section 3 - File Characteristics

- File Placement - Provide the CORPORATE OR SERVICE Node number and directory path of where the file(s) is to be placed. The requestor must have appropriate privileges to read and write files in this location.
- File Access Privileges: List the file access permissions (i.e. rwxrw----). These permissions will determine who has read, write, and execute privileges to the file(s).

Section 4 - Authorization of Action

- To Be Completed by DHSS Corporate or Service Node Administration Staff

3. Send completed Import Transmittal to DHSS

Send the completed Import Transmittal Form to the DHSS Corporate or Service Node Administration Team via electronic mail.

The Corporate or Service Node Administration Staff will ensure that the information is complete and accurate.

DHSS will not process an import request until both the Transmittal Form and media are in hand.

Upon reading the media, DHSS Corporate or Service Node Administration Staff will perform minimal QC, which consists of verifying that the file(s) and byte count(s) read were consistent with the Import Transmittal Form. DHSS will notify the requestor of the files placement in the specified location.

If necessary, DHSS Corporate or Service Node Administration Staff will coordinate the return of the media with the POC as indicated on the Import Transmittal Form.

Section A-7. Copying Files from the Corporate or Service Node to External Media

Corporate or Service Node users may periodically need a file(s) that exists within the Corporate or Service Node copied to external media and shipped to a third party for analysis or fulfillment of contractual obligations. DHSS is able to copy data to several types of external media. Choosing the type of external media is dependent on the size of the file(s) being copied and the technical abilities of the recipient organization.

Media Type	Maximum Size	Encryption Method	Notes
CD	700 MB	WinZip v11.2 or greater	Files larger than the max. size may be split or compressed to accommodate the size limitation
DVD	8 GB	WinZip v11.2 or greater	Files larger than the max. size may be split or compressed to accommodate the size limitation
USB Disk Drive	Dependent on the size of the drive	WinZip v11.2 or greater	Individual files must not be larger than 10GB in size.
LTO3 Tape	800 GB compressed	Storix or IBM TSM	
LTO4 Tape	1.6 TB compressed	Storix or IBM TSM	

Note: Thumb-drives are not permitted.

DHSS works with on-site DISA technicians to perform the data extractions. It is the requestor's responsibility to make arrangements on who supplies the media and how it gets returned to the owner. If the chosen type of external media is USB Disk Drive, a USB hard drive of adequate size must be supplied for the data export. In accordance with DISA security protocol, previously used USB hard drives will be scanned, wiped, and re-configured before being allowed into their complex. If a new, in the box, drive is supplied the time to create and ship the external media is much quicker.

Following are instructions for having a file(s) read to external media and shipped.

Notes:

- The Corporate or Service Node user/requestor must have the appropriate permissions to view and extract the requested file(s).
- The data recipient, also referred to as third-party, must have a valid Data Use Agreement (DUA) on file with the TMA Privacy Office covering receipt and use of the data being extracted.
- The amount of time it takes to copy the data to external media is dependent upon the size of the file(s), accuracy of information contained on the Export Transmittal Form, the number of requests for exports in queue, and approval from DHCAPE and DHSS Management. DHSS generally acts on data export transmittals in a "first-in, first-out" manner unless otherwise directed by DHCAPE.
- DHSS Corporate or Service Node Administration Staff will not manipulate (split or compress) files. Files to be copied to external media must be in their final format.

1. Complete an Export Transmittal form

Complete an Export Transmittal form by supplying the following information. The Export Transmittal Form may be found in Appendix A, entitled *Basic User's Guide for UNIX and SAS*, Attachment A-2.

Section 1 - Requestor and Shipment Information

Requestor Name - The Corporate or Service Node user requesting the data be cut to external media.

Requestor Company Name and DUA # - The Corporate or Service Node user company name and the Data Use Agreement (DUA) number which authorizes the work to perform extractions for the data recipient (note that the DUA # should match the DUA # that is listed on the users CE AARF).

Project and Justification for Export - List the Project details which require that data be written to external media and sent to the recipient.

FEDEX Account Number (for shipping) – Provide a Federal Express account number for shipment of the external media to the recipient. The account number may be provided by the Requestor or the Recipient. DHSS ships external media via Standard overnight delivery unless otherwise directed. Saturday delivery may be accommodated if the request is urgent but it is your responsibility to ensure that the recipient's location is open and someone is available to take receipt of the package.

Requestor Contact Info - The phone number and e-mail address of the requestor.

Shipment POC and DUA # - The third parties name, phone number, and address of where the tape should be shipped as well as the DUA number which authorizes receipt of the data.

Target Platform – Designate the system platform of the third party. What operating system will be used to read the media?

Media Type - Indicate the type of media to be created (CD, LTO3 Tape, LTO4 Tape, or USB Disk Drive).

Section 2 - File Characteristics

File(s) location - Provide the CORPORATE OR SERVICE Node number and directory path of where the file(s) is located.

File name(s) : line count : byte count - In this order, provide the file name(s) to be cut to external media, its line count, and file byte count.

i.e. If you have a file named myfile, with a line count = 54,980 and byte count = 1,354,900 the Export Transmittal would display the information like this: File name : line count : byte count	myfile : 54980 : 1354900
---	---------------------------------

Record format: record length and field names (flag PHI fields) - In this order, provide the file record format, and record length. Include a list of field names as specified.

i.e. If you have a file named myfile, with a fixed block record format and a record length = 76, the Tape Transmittal would display the information like this: File record format : record length	fb : 76
---	----------------

Section 3 – Media Characteristics

To Be Completed by DHSS Corporate or Service Node Administration Staff

Section 4 - Authorization of Action

To Be Completed by DHSS Corporate or Service Node Administration Staff

2. Send completed Export Transmittal to DHSS

Send the completed Export Transmittal Form to the DHSS Corporate or Service Node Administration Team via electronic mail:

- matthew.kapusta@absicorp.com
- Kathleen.Hutchinson.ctr@tma.osd.mil
- Martin.Shepherd.ctr@tma.osd.mil
- Fauzia.Jones.ctr@tma.osd.mil
- corinna.barnes@absicorp.com
- beth.pelletier@absicorp.com

The Corporate or Service Node Administration Staff will ensure that the information is complete and accurate, coordinate creation of the external media, perform minimal QC by checking the byte count(s), and ship the media to a third party as defined on the Export Transmittal Form.

3. If USB Disk Drive, Ship external media to DISA

- a. Drives must be shipped via Federal Express directly to DISA OKC. Two days prior to shipment, notify DHSS of plans to ship the external media.
- b. DHSS will respond to your notice with a work "ticket number" to include on the FEDEX shipping label. This information must be included on the shipping label or the drive may get inappropriately routed within DISA.
- c. Once you have a work "ticket number" the drive may be shipped to:

Defense Information Systems Agency (DISA) OKC
Attn: Chris Dozier
BLDG 3900
8705 Industrial Blvd.
Tinker AFB 73145
405-439-5600
Mark For/Regarding: DHSS OST (Lori Ponder)

- d. Notify DHSS that the drive has been shipped. Provide the FEDEX Tracking number and Serial Number of the USB Disk Drive in this notification.

Upon receipt of the USB Disk Drive by DISA, it will be prepared for data upload. When complete, the drive will be shipped to the recipient specified on the Export Transmittal. An email to the recipient will be sent once the package has been accepted by FEDEX to advise of shipping and tracking information.

Section A-8. Using PKZIP

PKZIP is located in `/usr/local/bin`. That directory needs to be in the PATH variable in your profile, otherwise you will need to call PKZIP with the full path name (`/usr/local/bin/pkzip`).

To check that `/usr/local/bin` is in your profile, sign onto WinSCP. By default, you should be in the `/trailhome/userid` directory (if not, navigate to that folder). Double click the file `“.profile”` (it may be grayed out); this will bring you to the edit mode. Check the PATH variable to ensure `/usr/local/bin` is listed. If it is not, go to the end of the variable string and add `“:/usr/local/bin”` then click the Save icon at the bottom of the screen.

To zip a file (this will place the zipped file in the directory you are in):

```
pkzip -add ZIPPED_FILENAME FILE_TO_BE_ZIPPED
```

Example:

```
pkzip -add results.zip results.txt
```

The file `results.txt` will be compressed and placed into the file `results.zip`.

To unzip a file (this will place the unzipped file in the directory you are in):

```
pkzip -extract ZIPPED_FILENAME
```

Example:

```
pkzip -extract results.zip
```

Uncompresses whatever file is in `results.zip` and places it in the directory you are in.

Password Protecting a File with PKZIP

When placing a file in a public area like `/temp`, you can password protect your file using `pkzip`.

1. First, password protect the file in your working directory. In this example, we will password protect the `results.out` file and copy it to `/temp`. The syntax of the command is:

```
pkzip -add -pass ZIPPED_FILENAME FILE_TO_BE_ZIPPED
```

You will be asked to enter a password twice. Notice that `pkzip` will leave your original file intact.

```

10.1.3.175 - PuTTY
[edwn65_sw]:/u/aliau > ls -l results*
-rw-rw----  1 aliau  staff      2944 Jun 10 12:41 results.out
[edwn65_sw]:/u/aliau > pkzip -add -pass results.out.zip results.out
PKZIP(R) Version 2.51 FAST! Compression Utility for AIX 4-15-1998
Copyright 1989-1998 PKWARE Inc. All Rights Reserved. Shareware Version
PKZIP Reg. U.S. Pat. and Tm. Off. Patent No. 5,051,745

Encrypting files

Creating .ZIP: results.out.zip
Password? ****
Re-enter password for verification
Password? ****

Adding File: results.out Deflating (72.6%), Encrypting, done.
[edwn65_sw]:/u/aliau > ls -l results*
-rw-rw----  1 aliau  staff      2944 Jun 10 12:41 results.out
-rw-r--r--  1 aliau  staff      956 Jun 14 08:01 results.out.zip
[edwn65_sw]:/u/aliau >

```

2. Move the zipped file into the /temp directory.
3. To unzip the file, copy or move the zip file into your own directory.
4. Unzip it using the correct password. The syntax is:

pkzip -extract -pass ZIPPED_FILENAME

```

10.1.3.175 - PuTTY
$ pkzip -extract -pass results.out.zip
PKZIP(R) Version 2.51 FAST! Compression Utility for AIX 4-15-1998
Copyright 1989-1998 PKWARE Inc. All Rights Reserved. Shareware Version
PKZIP Reg. U.S. Pat. and Tm. Off. Patent No. 5,051,745

Decrypting Encrypted files

Extracting files from .ZIP: results.out.zip
Password? ****

Inflating: results.out
$
$ ls -l results.out
-rw-rw----  1 wfunk  system      2944 Jun 14 08:09 results.out
$

```

Section A-9. Metadata for MDR Files

Metadata are available for most files that exist in the MDR and is accessible using the 'mdata' command.

What Is Metadata?

See Appendix B, Section 4 entitled *Accepting Data into the MDR* and Table 4-1 *Required Metadata for Information Files*.

Viewing Metadata for MDR Files

Prior to using the mdata command FOR THE FIRST TIME, users must perform the following two steps:

1. Make the following changes to their ".profile". To do this, through either PuTTY or WinSCP, go to /trailhome/*user_id* (e.g., /trailhome/jdoe).

For PuTTY, from the command line type: pico .profile (it may not appear when using the "ls" command but the file is there to edit)

For WinSCP, use the edit function to open the .profile (it may be grayed out but users should be able to edit).

Add the following lines and save to the same file name (.profile):

```
export DB2DBDFT=dbmdrp01
export DB2INSTANCE=perlxdb2
export INSTHOME=/db2/${DB2INSTANCE}
export LIBPATH=${INSTHOME}/sqlib/lib
PATH=${PATH}:${INSTHOME}/sqlib/adm:${INSTHOME}/sqlib/bin
export PATH=${PATH}:/apps/mdr/bin
```

2. In order to access the database, users must store an encrypted version of their password. This can be done by running the following command:

```
/apps/dis/bin/dmupwme
```

The script will prompt users to enter their current password twice.

Every time users change their password, this script must be run to store a new encrypted version of your password. Running the mdata command without an encrypted password may result in a locked account.

Once these steps are done, users should be able to run the mdata command by executing either of the following commands.

```
> mdata filename
```

or

```
> /apps/mdr/bin/mdata filename
```

where the list of files may be specified with either absolute or relative paths.

Following are examples:

```
/my/directory/> mdata /mdr/pub/pdts/detail/fy11/pdts.detail.fy11.txt.Z
```

```
/my/directory/> mdata /mdr/pub/caper/enhanced/fy11.sas7bdat
```

```
/mdr/pub/caper/enhanced> mdata fy11.sas7bdat
```

Please note that relative path names will not work in some cases due to discontinuities between the names of symbolic links and mount points within the MDR file system. Absolute path names are not subject to these issues and will always work.

Section A-10. The PICO Editor (Preferred for the Novice)

([http:// www.ncsu.edu/cc/essentials/managing_files/text_editors/pico_tutor/index.html](http://www.ncsu.edu/cc/essentials/managing_files/text_editors/pico_tutor/index.html))

PICO is a line-mode text editor used to create files, reports and letters. You will need a line-mode editor if you use your account on a non-X Windows computer.

Starting PICO

To start using PICO, enter 'pico filename' at the system prompt where filename is either the name of the file you want to edit (one that already exists) or the name of a new file you want to create. If you do not provide a file name, PICO will open a new file but it will be unnamed until you save it.

The screen for a new file will look something like this:



In the list of commands at the bottom of the PICO screen, caret (^) stands for the control (ctrl) key. '^G' means to hold down the control key and press the letter 'G'. PICO commands are always a combination of the control key and another key. After you enter a PICO command you do not need to press the return key.

Quitting PICO

Press '^x' to quit or exit the PICO editor. PICO will prompt you with a message asking if you want to save your changes. 'Y' saves the changes and 'N' quits PICO without saving what you've done since the last time you saved.

Entering Text

At the system prompt, type 'pico' to create a new file. You should see PICO in your window. The top line of your screen is called the status line. It shows what version of PICO you are using, the file name (it will say New Buffer if it hasn't been named yet), and whether or not you have made changes (Modified will be in the upper right corner of the PICO screen if something has been entered but not saved). At the bottom of the screen are two lines showing the commands available for your use.

Now that you have an empty file, you can start typing. PICO automatically starts a new line when you run out of room (called "wrapping text," "text wrap," or "autowrap") so you do not need to watch the screen while you type. Press [return] when you want to start a new line. If you want a blank line between lines of text or data, press [return] twice.

Saving the file

Now that you have a file with something in it, this is a good time to save your work. You should save your files often, if for no other reason than strange things can happen and sometimes do. The common sense rule is to save often enough so that if you lose your work you will not have much to re-do. Some people recommend saving every 15 minutes.

To save a file, use '^o', which stands for write out because you are writing what you have done to a file as output. When you press '^o', PICO will prompt you for the file name. If the file does not have a name yet, you will need to type one in. If the file does have a name, it will follow the file name prompt, and all you need to do is press [return].

You may also save the file during the process of quitting PICO. '^x' quits PICO after prompting you to save the file. Press '^Y' to save the file. Pressing '^N' will return the file to the state it was in the last time you saved it (if you had not saved the file during this editing session, the file will return to the state it was in when you opened it). If you alter a file and want to save the original version as well as the modified version, enter '^Y' to save the file. When you are prompted for a file name enter a new file name.

Editing in PICO

You can easily edit short files using only the following keys:

- [ret]: Inserts a new line in the file.
- cursor (arrow) keys: The four arrow keys move the cursor up, down, left and right.
- backspace/delete key: Deletes the character preceding the cursor.

Cutting text

Cutting or deleting text is a major component of any kind of editing. PICO gives you two ways to cut text: (1) cut a character at a time, or (2) cut a line at a time (unfortunately, you cannot cut a word at a time).

To delete a character, place the cursor on the character you want to delete and press '^d'. Pressing your keyboard's delete key (some keyboards label it backspace) will delete the character preceding the cursor.

To delete an entire line, place the cursor anywhere within the line and press '^k' (for kill or cut text). The entire line will be cut. If you change your mind about deleting the line before you delete another one, you may press '^u' to bring back the line. The restored line will be placed wherever the cursor is.

Pasting text

Since '^u' lets you restore the cut line wherever the cursor is and not just to wherever it came from, you may use '^k' and '^u' to "cut and paste" text. In PICO, you move blocks of text similar to if you were using a word processing package. You first need to mark (highlight) the text you want to move. Cut the text, move the cursor to where you want the text inserted, then paste it.

Position your cursor at the beginning of the first line of the text block you want to move. Press '^' (ctrl-shift-6 key). Move the cursor to the end of the block you want to cut. The text should then be highlighted. Once the block is highlighted, press '^k' to cut the text. Place the cursor to where you want the text placed, and press '^u' to paste. The text should then appear.

Reformatting text

To justify or reformat a paragraph (fill in gaps left by starting a new line) press '^j'. PICO defines paragraphs as text surrounded by blank lines or indentation. However, if you had a blank line between each line of text pressing '^j' would not affect the text.

If you do not like the result of the justification, press '^u' to "unjustify" the paragraph before you move the cursor outside the paragraph. Once you have justified text, the '^u' command function changes from undelete to unjustify. However, when you move the cursor from the justified paragraph, the '^u' command function returns to undelete. Therefore, if you need to unjustify the paragraph, you must do so before you move the cursor outside the paragraph.

To join lines that are separated by blank lines use '^k' to delete the blank line and '^j' to fill the paragraph.

Searching your PICO file

If you are proofreading a file by looking at a printout, it may be tricky to find the specific line you want to revise. An easy way to get to the right point in your file is to use PICO's search, or 'where is' command, which is '^w'. This command lets you enter a character(s) or word(s) to search for, and then moves the cursor to the first occurrence. PICO begins the search from the point in the file where the cursor is located. So, if the cursor is at the beginning of the second paragraph, the search begins at the beginning of the second paragraph.

To find a specific character or word, press '^w' (for where is). A black strip with the word 'search:' will replace the two lines of commands at the bottom of the screen. You should then type the character(s) or word(s) you want to find. This search command is not case sensitive. This search command is also not limited to finding only whole words. For example, if you were to tell PICO to find "th", it would find "that", "the", "they", and "thick", etc.

Using the spellchecker

PICO has a spellchecker that will check spelling in your text files.

To start the spellchecker, press '^t'. The PICO spellchecker compares the words in your file to words that are in its dictionary. When it finds a word that is not in its dictionary, it sends the prompt 'Edit a replacement:' followed by the misspelled word. If the word is correct, just press return. If the word is misspelled, you may change it by backspacing over it (to delete it) and then typing the correct word. You may also use the cursor and delete keys to edit parts of the word.

Inserting a file into PICO

To insert an existing file into the PICO file you are currently editing:

- Locate the cursor where you want to place the inserted file
- Press '^r'. After you press '^r', you will receive the prompt 'Insert file:'
- Type in the name of the file you want to insert and press return. The inserted file's contents will be inserted at the cursor.

This command does not delete or in any way alter the file that is to be inserted (a copy of the file is inserted).

If you change your mind about inserting the file after you have pressed '^r', when prompted for the file name enter any character string that does not correspond with a file. The system will attempt to process the command, but when it does not find a corresponding file it will cancel the command and your text will not be altered. You will, however, receive the message 'No such file:' followed by the character string you entered.

Control keys for moving around in a file

If for some reason you can not use cursor (arrow) keys, you may use the following commands to move around in your file.

- '^p' moves to the Previous line.
- '^n' moves to the Next line.
- '^f' moves Forward a character.
- '^b' moves Backward a character.

Clearing the display

If your display becomes cluttered (most likely because of interactive messages), you may clear or refresh it by entering '^l'. The messages are erased from your screen and the file you are working with remains.

Command list for PICO

The commands you can use in PICO are listed across the bottom of the screen. Remember, '^' symbolizes the control key. '^G' means to hold down the control key and press G.

- | | |
|----|--|
| ^G | Help. More information on the commands. |
| ^X | Exit PICO |
| ^O | Save a PICO file |
| ^J | Justify text within a paragraph. This command will fill in paragraphs that are missing, etc. |
| ^R | Insert an existing file into PICO. |
| ^W | Find a word or character string in the PICO file. |
| ^Y | Go back to the previous page. |
| ^V | Go to the next page. |
| ^K | Cuts the line of text where the cursor is located. |
| ^U | Uncuts the last text cut. |
| ^C | Gives you the exact location of your cursor within the file. |
| ^T | Run the spell checker. |

When you have selected ^O to save a file or ^R to insert a file, you will be prompted for a file name. You will also be given the following new options:

- | | |
|----|--|
| ^C | Cancels the command. |
| ^T | Gives you a list of files in your home directory. If you select a file that already exists, PICO will ask you if you want to overwrite the file. |

Section A-11. Basic VI Editor - A Beginner's guide to vi and ex

Beginning Your Editing Session

To edit a file	vi [filename]
To recover an editing session	vi -r [filename]

Notes on vi commands and modal editing

All vi commands are entered in command mode. To enter command mode, press the ESC key. Some vi commands cause vi to enter another mode. For example, the i (insert command) causes vi to enter insert mode after which all keystrokes are inserted as text. To return to command mode from insert mode, press the ESC key. The :set showmode command will cause vi to display the current editing mode in the lower right corner of the editing screen.

Controlling the Screen Display of Your Session

Repaint the current screen	{^!}
Display line #, # of lines, etc..	{^g}

Moving the Cursor

Beginning of current line	0 or ^
Beginning of first screen line	H
Beginning of last screen line	L
Beginning of middle screen line	M
Down one line	j, {return}, +
End of current line	\$
Left one character	h, {ctrl-h}
Left to beginning of word	b, B
Right one character	l, {space}
Right to end of word	e, E
Right to beginning of word	w, W
Up one line	k, -
Beginning of next sentence)
Beginning of previous sentence	(

Paging Through Text

Back one screen	{^b}
Down half a screen	{^d}
Down one screen	{^f}
Forward to end of file	G
Move cursor to specified line	line no.G
Up half a screen	{^j}

Special Pattern Characters

Beginning of line	^
End of line	\$
Any character except newline	.
Any number of the preceding character	*

Any set of characters (except newline) *

Searching Through Text

Backward for pattern	?pattern
Forward for pattern	/pattern
Repeat previous search	n
Reverse direction of previous search	N
Show <i>*all*</i> lines containing pattern	:beg,endg/pattern/p
Example	
:1,\$g/compiler/p	Will print all lines with the pattern compiler.
Substitute patt2 for all patt1 found.	:beg,ends/patt1/patt2/g
Example	
:%s/notfound/found/g	Will change all occurrences of 'notfound' to 'found'.

Creating Text

Append text after cursor	a
Append text after end of line	A
Insert text before cursor	i
Insert text at beginning of line	I
Open new line after current line	o
Open new line before current line	O
Take next character literally (i.e. control characters...) and display it	{^v}

Modifying Text

Change current word	cw, cW
Change current line (cursor to end)	C
Delete character (cursor forward)	x
Delete character (before cursor)	X
Delete word	dw, dW
Delete line	dd
Delete text to end of line	D
Duplicate text	(use yank and put)
Join current line with next line	J
Move text	(use delete and put)
Put buffer text after/below cursor	p
Put buffer text before/above cursor	P
Repeat last modification command	.
Replace current character	r
Replace text to end of line	R
Substitute text for character	s
Undo your previous command	u
Transpose characters	xp
Yank (copy) word into buffer	yw
Yank (copy) current line into buffer	Y

Making Corrections During Text Insertions

Overwrite last character	{delete}
Overwrite last word	{^w}

Ending Your Editing Sessions

Quit (no changes made)	:q
Quit and save changes	ZZ, :wq
Quit and discard changes	:q!

Using ex Commands From Within vi

Copy specified lines	:co, t
Display line numbers	:set nu
Disable display of line numbers	:set nonu
Move lines after specified line	:m
Read file in after specified line	:r filename
Review current editor options	:set
Review editor options	:set all
Set new editor option	:set option
Write changes to original file	:w
Write to specified file	:w filename
Force write to a file	:w! filename

Some Useful ex commands for use in vi

Some useful set options for your ~/.exrc file:

:set all	Display all Set options
:set autoindent	Auto magically indent following lines to the indentation of previous line.
:set ignorecase	Ignore case during pattern matching.
:set list	Show special characters in the file.
:set number	Display line numbers.
:set shiftwidth=n	Width for shifting operators << and >>
:set showmode	Display mode when in Insert, Append, or Replace mode.
:set wrapmargin=n	Set right margin 80-n for autowrapping lines (inserting newlines). 0 turns it off.

Section A-12. Changing Your Corporate or Service Node Password

AIX passwords must be changed every eight weeks, approximately 55 days. Upon login the system will display the number of days remaining to password expiration. Follow the instructions below to change your password before the expiration date. If your password is not changed within the 55 days, your account will be automatically locked. If this occurs, follow the appropriate instructions below.

As of March 2010, security guidelines for the SCE dictate that AIX passwords must be:

- ✓ a maximum of 2 repeated characters
- ✓ a minimum of 2 characters not found in old password
- ✓ a minimum of 4 alphabetic characters
- ✓ a minimum of 4 non-alphabetic characters
- ✓ a minimum of 15 characters in length

Other password rules:

- Password history is set to 10 which means that the system keeps track of your last ten passwords and will not allow your new password to contain more than two characters in common with any one of the last ten passwords.
- Accounts will be locked after 3 unsuccessful login attempts. Unsuccessful login attempts will continue to accumulate until the maximum of three is reached. If your account is locked because of too many unsuccessful login attempts, contact the MHS Help Desk at 800-600-9332, option #7 (EIDS Help Desk Support).
- Upon successful connection to the system, a legal warning will be displayed which states that by continuing to login to the server you consent to monitoring of your activities.
- Upon successful login, the system will display the date and time of Last Successful Logon. For security purposes verify this date and time to ensure it matches your records of last logon. If you did not log on to the system at that date and time notify the MHS Help Desk at 800-600-9332, option #7 (EIDS Help Desk Support) as soon as possible.
- If you have access to Purchased Care systems (TED, PCDW, HCSR, etc.) and/or access to CDM, be aware that these systems have separate password control managers - one for Purchased Care systems, one for CDM, and one for the SCE. When your password is changed in the SCE, it will not alter/update/change your password on those systems. As of March 2010, the password control managers for Purchased Care and CDM have not converted to use of a minimum fifteen character password. They are still requiring a minimum eight character password.

We do not recommend changing your password via the corporate or service node (i.e., using the ssh command). The following should be performed:

How to change my password. To change your password, connect directly to the password control manager to change your password.

1. Invoke PuTTY by double-clicking on the icon.
2. At the PuTTY Configuration screen enter the **IP Address** of the TBCPM server under *Host Name (or IP address)* and specify the **Port** number to be 22:

TBCPM Node:	2.15.123.5 (OOB access)
TBCPM Node:	152.229.239.47 (non-OOB, *.mil address only)

3. Click on **SSH** under *Protocol*.
4. On the left-hand side of the window, under *Category, Connection*, click on **SSH**. Ensure that you have:
 - Preferred SSH protocol version = **2**
 - Preferred encryption algorithm = **3DES**
5. Click on **Session** under *Category*. Enter a 'nickname' in the *Save Sessions* field, and click on **Save**. Doing this will prevent you from having to enter this information each time you log on.
6. Double-click on the *Saved Sessions* name OR click the *Saved Sessions* name, **Load**, and then **Open**.
7. When prompted, enter your User ID.
8. Follow the prompts to enter your current password and new password. DoD strong password requirements apply to these servers so make sure to follow the strong password rules (described above).
9. **Once your password has been updated on the TBCPM it will take approximately 20-30 minutes to propagate to the SCE nodes. Do not attempt to connect to the SCE before the system has had time to propagate your new password or you risk the possibility of exceeding the maximum number of unsuccessful login counts.**

If you are unable to connect to the TBCPM server or after 30 minutes your new password has not propagated to the SCE nodes, please contact DISA OST 405-739-5600, option #6. You MUST provide the following information to DISA OKC.

Ticket Categorization	ROUTINE
Project/Application Name*	MDR/SCE
Environment**	prod
Operating System (AIX, SUN, Windows, or Linux)	AIX
CSHIP Name	UTINIP23 (node 2130, Corporate Node) Or UTINIP24 (node 2131, Service Node)
Description of Request or Problem	Reset password for userid_here on node node_number_here
Impact Description	Can not log onto system
Will a DHSS Scheduled Maintenance checklist be submitted?	No
Date problem first noted	
New requirement? (Server, Zone change, DMZ, URL, IP change, IP Config change)	No
User Full Name, User ID, Email, and Phone Number	
Source and Destination IP (if Comm. Related)	NA
Due Date and Time	Should be 24 hours from when ticket is submitted

*A separate ticket for each project/application is required.

** Other rarely used options are Dev, DevTest, ProdTest, Pre-Prod

Section A-13. Commonly Used UNIX Commands

Following are some of the basic commands that you will need in the UNIX environment. Commands are placed in quote marks ("). These marks are NOT typed when using the command.

Command Reference Table

● ls

The "ls" command lists files in a directory. There are many options you can use with the "ls" command. For example "ls -a" will list ALL of the files in a directory (files and directories whose name begin with a period are considered hidden files). "ls -al" will list ALL files in LONG format. Here is an example directory listing:

```
www:~> ls -laF
total 34
drwxr-xr-x  4 root  other    2048 Sep 24 11:25 ./
drwxr-xr-x 102 root   root     2048 Sep 24 11:24 ../
-rw-r--r--  1 root  other     384 Jan  6 1998 .bashrc
-rw-r--r--  1 root  other     383 Jan  6 1998 .cshrc
-rw-r--r--  1 root  other     706 Jan  6 1998 .defaults
-rw-r--r--  1 root  other    1858 Jan  6 1998 .emacs
-rw-----  1 root  other    2797 Jan  6 1998 .history
-rw-r--r--  1 root  other     137 Jan  6 1998 .login
-rw-r--r--  1 root  other     138 Jan  6 1998 .logout
-rw-r--r--  1 root  other     232 Jan  6 1998 .mailrc
drwx-----  2 root  other     512 Jan  6 1998 Mail/
drwxr-xr-x  2 root  other     512 Jan  6 1998 bin/
```

In this example, the first block of each row (-rw-r--r--) shows the type and permissions for an individual file within your current directory. The first column tells you the type of file: '-' means it is a normal file, 'd' means it is a directory, and an 'l' means it is a link to another file (much like a shortcut in Windows). The next nine positions show the file's Read, Write, and Execute permissions in blocks of three. The first three characters (often 'rw-') are the permissions for the owner of the file, the second three are group permissions, and the final three are permissions for anyone else besides the owner and anyone in the group.

The next column is a number representing how many physical links to the directory or file exist on the file system. Your home directory, '.', will usually contain 4 links to it: a link from /home/yourhomedir pointing to your directory, the pointer '.' which resides within your directory, and the '.' pointers from within your 'Mail' and 'bin' directories. Files generally have one link to them due to the fact that directories cannot link to files specifically. Notice that the directory up one level, '..', contains a large number of links (102) due to the number of home-directories that reference it as '..'.

The next four columns contain the name of the owner of the file (equivalent to the first three 'rwx' permissions), the group owner (second three 'rwx'), the file size, file date, and file name. Note that by using the '-F' flag (must be a capital F), directories are marked with the / symbol, and the / is not actually part of the directory name. Also, files marked as executable are shown with the '*' symbol following the name (only when the -F flag is set).

● cd

The "cd" command is used to change directories. The "cd /" will take you to the root directory of the file system tree; "cd /usr" will take you to the directory named 'usr' that is located off of the root directory; "cd Mail" will take you into a directory called 'mail' off from your current directory (note the lack of '/' before the directory name); and "cd .." will take you to the parent directory in

the file system tree. Some command-line shells, such as "bash" or "tcsh" expand the ~ symbol to mean a person's home directory. You could then either type "cd ~" to change back to your home directory, or "cd ~anotheruser" to go into another user's home directory.

- pwd

The "pwd" command prints/outputs your present working directory to standard output.

- mkdir, rmdir

These commands are used to create and remove directories. The "mkdir class" will create a directory called class in your current directory. Whereas "rmdir class" will delete the directory named class. Note that "rmdir" only works on directories that do not contain any files.

- cp

To copy a file, use the "cp" command. The syntax is "cp *source destination*", where *source* is a source file and *destination* is either a file name or directory in which to place the file. For example, "cp /usr/local/seminar.c ." will copy a file located in /usr/local named 'seminar.c' to '.' which is the symbol that stands for your current directory. "cp /usr/local/seminar.c my.c" will copy the 'seminar.c' file to your current directory under the name 'my.c'.

- mv

The "mv" command is used to move *and/or* rename a file. "mv my.c first.c" will rename a file called 'my.c' to 'first.c'. Assuming that 'class' is a directory, "mv my.c class" would move the file 'my.c' into the 'class' directory. If 'class' is a file, this operation will instead delete 'class' and then rename 'my.c' as 'class', which is probably something you didn't want. You can also rename and move at the same time. For example, "mv my.c class/first.c" would move the file 'my.c' into the 'class' directory and rename it to 'first.c' all in one step.

- rm

The "rm" command deletes, or removes, files from the files ystem. Typing "rm my.c" would delete the file 'my.c'. You can also use wildcards. For example, "rm my*" will delete every file whose name started with the word 'my', including 'my.c'. Unlike Windows, these wildcards can appear anywhere in the file name, and do not need to be confined to the standard 8.3 notation used by MS-DOS. Directories and their contents can be deleted by using the '-r' flag which stands for recursiveness. For example, "rm -r class" would delete ALL files and directories under 'class' and 'class' itself regardless if the directory is empty or full.

- cat, less, more, head, tail

These commands are used to view the contents of files. "cat" displays the entire file on the screen, regardless if your terminal can view everything at once (the top portion scrolls off, but can be retrieved by scrolling back in a window or sometimes by holding down the 'Shift' key and pressing 'Page Up'). "less" and "more" both display the contents of a file one full screen at a time. "head" is used to display the first few lines of a file, and "tail" is used to display the last few lines of a file. For example, "tail -25 my.c" displays the last 25 lines of the file 'my.c'. "cat first.c" would display all of 'first.c', and "more first.c" will display the file 'first.c' one screen at a time.

- grep

Search a file for a particular pattern by using the "grep" command. "grep" stands for Get Regular Expression Pattern. This command searches a file for all lines matching a particular pattern and prints those matching lines on standard output. For example, "grep fun my.c" prints every line of the file 'my.c' that contains the word 'fun'.

- man

The "man" command brings up the UNIX Manual Pages for a particular command. For example, to learn about the rest of the options for the "ls" command, type: "man ls"

- w, who, whoami, id

These commands are used to find out the list of users currently logged into the system and what they are doing. "w" provides slightly different output than "who". "whoami" returns the username of the person currently logged in. "id" prints your User ID, and Group ID, and a list of all the groups you have access to.

- chmod

The "chmod" command is used to change the permission bits, called mode, on a file or directory. Only the owner of a file or directory and the superuser can change the permission bits/mode. See the "ls" command for information on viewing a file or directory mode.

Every file and directory is assigned nine permission bits that comprise the mode. The mode is used to determine what operations may be performed on a file and by whom. The mode consists of Read, Write, and Execute bits in blocks of three (Execute is also called "search" when referring to a directory): one block for the owner of the file or directory, one block for the group that the file or directory belongs to, and one block for others. Each user will fit into only one of the three blocks/categories.

For files, the read bit allows the file to be opened and read. The write bit allows the contents of the file to be modified or truncated. The execute bit allows an executable file to be executed.

For directories, the combination of read and execute (aka "search") bits allows the contents of the directory to be listed. The combination of write and execute bits allows files within that directory to be created, deleted, and renamed. Having only the execute bit will allow the directory to be entered but not have any of its contents listed.

File or directory modes may be changed using octal notation or symbolic format. The octal notation format is described below. The basic syntax for the "chmod" command is:

```
chmod <octal or symbolic notation of read, write, execute permissions> <file or directory name>
```

The octal notation format sets file or directory permissions based on three octal numbers. The first number defines access for the user, the second number for the group, and the third number defines access for others. Each of the three numbers is a combination of permission bits. The octal notation is between 0 and 7.

Use the UNIX command CHMOD to change access permissions by summarizing the numerical values for Owner, Group and Other.

Digit	Permissions
0	None
1	Execute only
2	Write only
3	Write and execute
4	Read only
5	Read and execute
6	Read and write
7	Read, write, and execute

Examples:

```
#1) chmod 770 tedn.sas - allows owner and group to have read/write/execute privileges, other no privileges
#2) chmod 764 tedn.sas - allows owner read/write/execute, allows group read/write only, allows other read only
```

Using the "ls -l" command, example #1 and #2 above would appear as such:

```
#1) rwxrwx--- example1 groupname 2567 Sep 10 12:15 tedn.sas
#2) rwxrw-r-- example1 groupname 2567 Sep 10 12:15 tedn.sas
```

- ps

The "ps" command is used to find the Process Status of all processes currently running on the machine. Typing "ps" without any options lists all programs currently running in your process group. "ps ux" or "ps -ef" lists all of the processes on the machine (Some UNIX versions prefer

one method over the other. If one way does not work, try the other). Combining the "ps" and "grep" commands through a pipe can give you a list of all the processes you have running, and can be done like this:

```
"ps aux | grep yourusername"
```

The '|' symbol, called a pipe, takes the results of the first command (in this case, "ps -aux") and uses it as input to the second command ("grep yourusername"). Let's take a look at an example:

```
winds:/dsk0> ps ux
USER    PID  %CPU  %MEM  VSZ  RSS  TTY  STAT  TIME  COMMAND
root     1  0.0  0.1 1048  112  ?    S     0:03  init [3]
gandalf 521  0.0  0.0 1652   0  tty2  SW    0:00  [bash]
gandalf 652  0.0  0.7 1668  672  tty4  S     0:00  -bash
gandalf 672  0.0  0.0 1516   0  tty4  SW    0:00  [startx]
gandalf 677  0.0  0.0 2224   0  tty4  SW    0:00  [xinit]
gandalf 4481 0.2  1.6 4104 1560 pts/0  S     0:00  vi commands.html
gandalf 4452 0.0  1.0 1652 1012 pts/3  S     0:00  -bash
gandalf 4545 0.0  0.9 2496  936 pts/3  R     0:00  ps ux
```

The first column contains the user ID of the owner of that process. The second column contains the PID, or Process Identification number. The next two columns show the percentage of CPU Time and Memory the process has consumed during its entire running life. The next two columns show the Virtual Size of the program (total size of all memory in use) and how much of that memory is currently resident in the computer at the moment. Thus, the RSS number is usually much less than VSZ, because data are either shared, or is marked unused and are swapped to disk to free up room for other processes to use resident memory.

TTY shows which terminal the process is currently running on. Usually, tty1 through tty6 are processes controlled by a user at the main console (ALT-F1 through F6 to switch), and pts/# are processes from either inside X-Windows or through telnet in the network. STAT corresponds to the type of process status running at the time: 'R' means the process is currently active (as is the case for our "ps" command gathering the process data), 'S' means the process is sleeping, 'W' means the process is waiting for a signal to trigger swapping from disk and back into memory (note the 0 Resident Set Size), and 'Z' stands for a zombie process (see below). TIME shows the total amount of time the process has taken up CPU. In this case, each process except 'init' has taken up trace amounts of CPU, while 'init' has taken 3 seconds since the computer was started.

The last column of the "ps" command output contains the name of the process. The name can be represented in several different ways depending on the state of the process. If the name begins with a '-' symbol, such as '-bash', then it is recognized as a login shell. If the name is surrounded by []'s, then the process is currently swapped out of memory to disk (with an RSS of zero).

Zombie Processes. Processes marked 'Z' occur during a coding error on behalf of the programmer to not properly *wait* for one of its children to exit after a *fork* call in the C language ("man" pages are available for both of these functions). Such processes are marked <defunct> and will only terminate when their parent process (PPID) exits.

● kill, killall

Force a process to exit or terminate by using the "kill" command. This command is used to send signals to processes, most commonly the signal to kill a process (hence its name). Looking back at the "ps" example, to kill the "vi" process, you can type "kill 4481". Only programs that do not block the Terminate signal can be killed in this fashion. You instead must specify the "kill" command using a '-9' as the first argument to the prompt. For example, to kill the unused, swapped out 'bash' process, type:

```
"kill -9 521"
```

The "killall" command behaves in the same way as "kill", only each process matching the name you give it will be sent the signal. To kill all of your "bash" programs (and consequently kick yourself back to the login prompt), type:

```
"killall -9 bash"
```

Note: If you own a process that is using close to 99% of the CPU, it is generally a good idea to "kill -9" it, as it most likely won't respond to normal signal handling. The system PID 1, "init", can never be killed.

Note: Do not use kill to kill a SAS job, use the sasstop command.

● at

The "at" command reads from standard input the names of commands to be run at a later time and allows you to specify when the commands should be run. The "at" command mails you all output from standard output and standard error for the scheduled commands, unless you redirect that output. It also writes the job number and scheduled time to standard error. When the "at" command is executed, it retains the current process environment. It does not retain open file descriptors, traps, or priority. The syntax for the "at" command is:

```
at [ -c | -k | -s | -q Queue ] [ -m ] [ -f File ] { -t Date [Time [ Day ] [Increment ] }
```

For example, if user *jdoe* wants to run a sas job called *jobname.sas* from a fictitious common directory at 11:30pm on August 15th, the command would be as follows:

```
/common/jdoe/jobname.sas |
  at 2330 Aug 15 <enter>
  sas jobname.sas <enter>
  <ctrl-d>
```

For more information about different options and techniques on the formation of the "at" command, reference the man pages.

● compress

The "compress" command compresses data using adaptive Lempel-Zev coding to reduce the size of files. When possible, a compressed file replaces the original file, specified by the file parameter, with a .Z appended to its name. The compressed file retains the same ownership, modes, and modification time of the original file. If no files are specified, the standard input is compressed to the standard output. If compression does not reduce the size of a file, a message is written to standard error and the original file is not replaced. Files being compressed must have correct permissions to be replaced. For example, to compress the 'foo' file and write the percentage of compression to standard error, type:

```
compress -v foo
```

The foo file is compressed and renamed foo.Z.

For more information about different options and techniques on the formation of the 'compress' command, reference the man pages.

● uncompress

The "uncompress" command restores original files that were compressed by the "compress" command. Each compressed file specified by the file parameter is removed and replaced by an uncompressed copy. The uncompressed file has the same name as the compressed version but without the .Z extension. If the user has root authority, the expanded file retains the same owner, group, modes, and modification time as the original file. If the user does not have root authority, the file retains the same modes and modification time, but acquires a new owner and group. If no files are specified, standard input is expanded to standard output. For example, to uncompress the foo.Z file, enter:

```
uncompress foo.Z
```

The foo.Z file is uncompressed and renamed foo.

Section A-14. UNIX File Naming Conventions

Absolute Naming

Within the UNIX directory structure there are two ways to name any file: relative naming and absolute naming. An absolute name, or absolute path as it is often called, specifies exactly where in the file system the particular file is. It tells the whole name of the file, starting at the root of the file system. An absolute name starts with /, the root, and names each directory along the path to the file, separating the directories with /. This is very similar to DOS, except for the direction of the slash and the fact that there is no disk drive designation. As an example, the absolute name for your mailbox might be /home/iris2/class9/mbox. The 'pwd' command always reports an absolute pathname.

Relative Naming

The second way to name a file in UNIX is with a relative name. Whereas an absolute name specifies exactly where in the file system a particular file exists, a relative name specifies how to get to it from your current directory. The look of a relative name may vary a lot. Depending on your starting directory there are a number of paths to a particular file.

In the simplest case, just naming a file in your current directory is a relative name. You are specifying how to get to this file from your current directory, and the path is to just open the file in the current directory.

When using relative paths, the special directories '.' and '..' that are contained in every directory are used frequently. Recall that '.' specifies the directory itself, and '..' specifies its parent. So, if the file mbox is contained in your current directory, naming the file with ./mbox and mbox are equivalent. The special directory '..' is used to name a directory at the same level in the tree as your current directory, that is, a sibling of your current directory. The following example illustrates using '..' to look at a sibling directory.

```
% pwd
/home/iris2/class9
% ls
NewBibliography.refer  bibs          mbox
ShortFile              bin           src
baby.1                 ig.discography  unix.refer
% cd bin
% ls
pwwgen
% ls ../src
helloworld.c  pwwgen.c
```

Short-cuts for File Naming

Since certain file naming patterns are used over and over, UNIX provides some short-cuts for file naming. Actually, it is the shell that provides these, but the distinction is not critical at this point. In particular, very many file accesses are either to your own home directory or to the home directory of another user. To make it easier to point to these places, the ~ character is used. Alone, ~ refers to your home directory. So the file ~/mbox refers to the file mbox in your home directory. Likewise ~ username refers to the home directory of that particular user. So, ~dickson/mbox refers to the file mbox in the user dickson's home directory.

File Naming Limitations

UNIX allows you great flexibility in naming your files. Older System V Release 3 systems limited the length of a file name to 14 characters. Berkeley Unix systems, as well as newer versions of System V have substantially relaxed this limitation. Many systems allow the name of individual files to be up to 256 characters, and the maximum absolute pathname to be about 1023 characters. This means that files can be given meaningful names quite easily. Also, since UNIX is sensitive to the case of the file names, you can use mixed-case names to add clarity. While long, meaningful names can be quite nice, it is also possible to go overboard with file naming. So, try to give your files meaningful names, but try not to overburden yourself or others that have to access the files with overly long names.

File Name Extensions

While UNIX does not actually have the same notion of a file extension as is found in some other systems, notably DOS, many user and applications programs behave as it did. UNIX does not consider the '.' character any differently than any other character in a file name. However, applications programs often use it to add an extension to a file name that specifies something about the contents of the file. These extensions sometimes tell what programs were used to create a file. If more than one was used, and is needed to decode the file, multiple extensions are used. Typically, the extension will tell what language the data in the file is in. A good example of this is the C compiler. It assumes that its input files will have an extension of '.c'. Its executable output generally has no extension, unlike DOS which uses an .EXE extension for executables. If we have a program called hello.c, its executable version is likely to be called just hello.

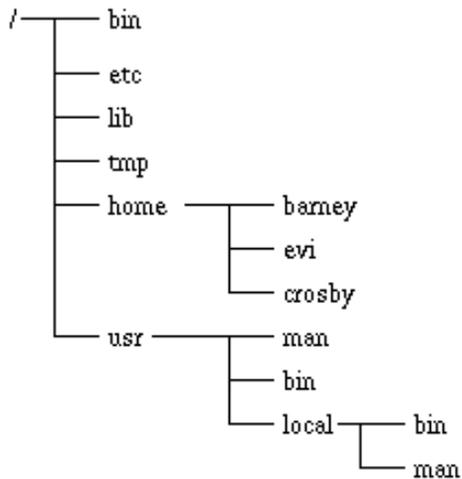
Section A-15. The UNIX Directory Tree

Files in UNIX are stored in directories, which are organized into a tree type configuration. At the top of the tree is the root, called /. A sample directory tree is shown below.

Locations in the directory tree are called paths, and are specified as a list of directories separated by a '/'. Barney's home directory, for instance, is in the home directory, which is in the root directory, and therefore the path is "/home/barney".

If you leave off the leading "/", the path is assumed to start in the directory you are currently in, for instance if you were in "home", "barney/songs" would be the directory songs contained in Barney's home directory. You can also use "..", which specifies the parent directory of the one you are in "../etc" from home would be the "/etc" directory.

There are a few standard directories you will find in pretty much all UNIX systems.



<i>/bin</i>	This contains the basic system commands.
<i>/etc</i>	This contains system configuration files and programs used for administrating the system.
<i>/lib</i>	This contains the system libraries.
<i>/tmp</i>	This is used to store temporary files.
<i>/usr/bin</i>	This contains all the commands not in /bin.
<i>/usr/man</i>	This contains manual pages for programs.
<i>/usr/local</i>	This contains local programs, that were installed by your sysadmin and not included with the original system. In particular, /usr/local/bin is local binaries and /usr/local/man is local man pages.
<i>/home</i>	The location of this varies greatly from system to system, but somewhere on the system will be a place where all the home directories are, including yours.

Getting Around Directories

You have been given a directory in which you can store your personal files, called your *home directory*. When you log in to the system, this is where you start off. You probably don't have any directories to start off with. If you want to create a directory underneath your home directory, use the *mkdir* command. For instance, to create a directory to hold your programs, type '*mkdir programs*'.

Now you have a directory you can get into with the *cd* command. For instance, to get into your *programs* directory, type '*cd programs*'. To get back to your home directory from anywhere, simply type '*cd*'. To go up a directory, type '*cd ..*'.

If you want to copy or move a file into a directory, use the *cp* or *mv* command as normal, but instead of specifying a destination file, specify a directory. For instance, if you type '*cp helloworld.c programs*' from your home directory, it will copy the file *helloworld.c* into your *programs* directory.

To remove a directory, use the *rmdir* command. Note that the directory must be fully empty to do this. To remove your *programs* directory, change to that directory using the '*cd*' command and type '*rm **'. This deletes all files in that directory so make sure you are in the right place! You can find out where you are by typing '*pwd*'. Now that all files have been deleted, you can delete the directory. Go back to your home directory and type '*rmdir programs*'.

Section A-16. Resource Considerations (Getting More Workspace)

There are far fewer resource constraints in the UNIX environment than in the mainframe environment in terms of space. UNIX System Administrators have monitoring tools that can tell them when space limitations are of concern and can expand the area within which your SAS programs or data reside.

Please notify the DHSS Corporate or Service Node Administration Team if you anticipate any large jobs that would obviously "exceed" the workspace capacity.

Attachment A-1: Import Transmittal Form

This form is intended for data imports via tape or CD-ROM to the CORPORATE OR SERVICE Nodes.

Date:

Section 1 - Requestor Information

Requestor Name:					
Requestor Company Name and DUA#:					
Requestor Contact Info:	Phone number:				
	E-mail:				
Return the Media(s)? Yes () No () If yes, please supply the POC for receipt of media return, along with their address and phone number.	POC Name:				
	Address:				
	Phone:				

Section 2 - Media Characteristics

Media Type:	CD ()	DLT ()	IBM 3480 ()	IBM 3490 ()	LTO ()
Total Number of DVDs, Tapes, USB Disk Drives:					

CDROM/DVD/USB Drive:

Contents:	
-----------	--

Tape:

Application used to create the tape (i.e. tar, ReelExchange, NTBackup, etc):					
Data Format of the Tape(s):	ASCII ()		EBCDIC ()		
Label Type:	ANSI ()	EBCDIC ()	UNLABELED ()		
File name : record format : block size : line count : record length : logical volume serial number					

Section 3 - File Characteristics

File Placement:	
File Access Privileges (i.e. rwxrw---):	

Section 4 - Authorization of Action – To Be Completed by DHSS Corporate or Service Node Administration Staff

Transmittal Reviewed and Approved By:	
---------------------------------------	--

Attachment A-2: Export Transmittal Form

This form is intended for use when data exists on the Corporate or Service Nodes and needs to be copied to tape, CD-ROM, DVD, or USB Disk Drive and sent to a third party.

* Date:	
---------	--

Section 1 - Requestor and Shipment Information

* Requestor Name:					
* Requestor Company Name and DUA #:					
* Requestor Contact Info:	Phone number:				
	E-mail:				
* Project and Justification for Export:					
* FEDEX Acct No. (for shipping)					
* Shipment POC:	Name:				
	Address:				
	DUA #:				
	Phone number:				
	E-mail:				
* Target Platform (i.e. Win7, XP, NT, UNIX, OS/390):					
* Media Type:	CD ()	DVD ()	USB ()	LTO3 ()	LTO4 ()

Section 2 - File Characteristics

* Node Name:	
* File(s) Location (directory)	
* File name(s) : line count : byte count:	
* Record format : record length and field names (flag PHI fields)	

Section 3 - Media Characteristics - To Be Completed by DHSS Corporate or Service Node Administration Staff
CD / DVD / USB Disk Drive:

Total Number of CD(s)/DVD(s), USB Disk Drive:	
Application used to create CD(s)/DVD(s):	
Application(s) used to transfer and encrypt USB Disk Drive(s).	
CD(s)/DVD(s)/Disk Drive Contents:	

LTO3 or LTO4 Tape:

File name(s): record format : block size : record length : logical volume serial number			
Data Format of the Tape(s):	ASCII ()	EBCDIC ()	
Label Type:	ANSI ()	EBCDIC ()	UNLABELED ()
Application used to create the tape(s):			

Section 4 - Authorization of Action – To Be Completed by DHSS Corporate or Service Node Administration Staff

Incoming Transmittal Reviewed and Approved By:	
Outgoing Transmittal Reviewed and Approved By:	

Appendix B. MDR File Naming Conventions for the Corporate and Service Nodes

Table of Contents

Section B-1: Introduction

- Background
- Purpose of the Document
- Scope

Section B-2: Overview of the MDR

- Operational Concept
- Technical Architecture
- Custodianship

Section B-3: Storage and MDR File Naming Convention

- Storage Convention
- File Naming Convention

Section B-4: General Procedures

- Accepting Data into the MDR

Section B-5: PUB Data Types

Section B-6: REF Data Types

Section B-7: Acronyms and Abbreviations

Section B-1: Introduction

This section describes the Military Health System (MHS) Data Repository (MDR) data sets that are accessible to the Corporate and Service Nodes.

Background

The MDR data sets comprise an enterprise repository consisting of workload, cost, demographic, population and reference data for the MHS. The data are hosted on an IBM System p5 Server at the Defense Enterprise Computing Center (DECC) OKC in Oklahoma City, Oklahoma.

Purpose of the Document

This document describes the File Management Conventions for the MDR data sets located at DECC OKC accessible to the Corporate or Service Nodes. The document's purpose is:

- To serve as reference for the custodians and users of the data
- To describe the operational context where rules apply
- To promote usability and reliability of the MDR data sets

And more specifically:

- To provide the file naming convention (Section B-3)
- To provide the framework for inventory of the MDR files (Section B-5 and B-6)

Scope

This document applies only to the MDR data sets residing at the DECC OKC on the IBM System p5 Server platform.

Section B-2: Overview of the MDR

Operational Concept

The MDR is the central repository for MHS corporate data. The data are quality assessed, of known origin, and complete. The MDR data are received in a known raw or pre-processed state:

- According to a defined periodicity or update cycle;
- Processed using known, tested software, with identified business rules;
- Quality controlled, documented, and reviewed; and
- Released for specified use.

Technical Architecture

The MDR is a compilation of ASCII flat files and SAS data sets. Much of the processed data resides as SAS data sets and takes advantage of SAS procedure and library functions. The MDR has no user interface in the traditional sense. It is intended for high-level corporate analysis and as a source to other systems.

MDR data flows from one of three sources:

- From source systems in the field
- From other servers located at the DECC OKC
- From other MHS organizations that govern reference data

Custodianship

The custodianship of the MDR resides with the DHSS Program Office. Access to MDR data sets visible through the Corporate or Service Node is granted in the following manner:

1. Potential users obtain approval to access the Corporate or Service Node from the Access Authority.
2. Potential users who are Non-DoD employees apply for ADP-II Clearance with the MHS AIS Security Office.
3. Potential users submit a Data Use Agreement (DUA) and other required documents or data requests to the TRICARE Management Activity (TMA) Privacy Office requesting access to the MDR data sets.
4. The TMA Privacy Office approves/denies DUA to specified MDR data sets.
5. Potential users obtain Information Awareness Certification.
6. Potential users submit an OKC MDR Password Authorization Form to the DHSS Corporate or Service Node Administration Team requesting access to specific MDR data sets as referenced by their approved Data Use Agreement.
7. CACs are required to access the Corporate and Service Nodes.
8. A DD2875 must be completed and turned into DHSS Access.
9. DISA creates the user account.
10. DHSS Corporate or Service Node Administration Team grants specific file system access.

Section B-3: Storage and MDR File Naming Convention

This section provides an overview of the MDR data file naming convention, and detailed descriptions of each element of the file naming convention. This file naming convention must be used for all data available to the general public (processed and reference) that is stored in the MDR.

Storage Convention

The MDR is partitioned into two Data Storage Areas (DS_Areas): 'pub' and 'ref'. The Data Storage Areas are directory structures within which defined states of data reside; they identify what kind of data the files contain.

'pub' - This Data Storage Area is for storage of accepted MDR data. This contains the most recently processed and released candidate MDR data. In most cases, the 'pub' area does not grow as each updated file replaces an existing file unless it is the first Data Type for a new fiscal year to be placed in 'pub'. However, for some Data Types, there is a new file added monthly.

'ref' - This Data Storage Area is for storage of the most recent reference data required for processing. The 'ref' area does not grow as each updated file replaces an existing file unless it is the first reference file of its kind for a new fiscal year to be placed in 'ref'.

File Naming Convention

All MDR files will be stored using a naming convention that begins with '/mdr'. The operator then must classify each file. The MDR data are classified into one of the Data Storage Areas (DS Area for short): 'pub' or 'ref'.

Several file types reside in the MDR. The standard File Types are:

- *.txt for ASCII text or flat files – txt is used for files that are too large to store efficiently as SAS data sets
- *.sas7bdat for SAS data sets – most of the processed data are stored as SAS data sets
- *.fmt for SAS format files – reference files that are used during SAS processing

While different Data Storage Areas and Data Types will have slightly different conventions, in general the naming convention for 'pub' files (public) and 'ref' files (reference) are:

- /mdr/DS_Area/subject[/period]/subject[.period][/sas_name].file_type
- /mdr/DS_Area/subject[.period][/sas_name].file_type.

Each of these segments are described below.

mdr

All files that are part of the MDR must be in the /mdr file system.

DS Area

The Data Storage Area or DS Area is required for all File Types.

The Data Storage Area identifies whether the file contains processed data or reference data. Valid values for the DS Area are shown in Table 3-1.

Table 3-1. MDR Data Storage Areas

Data Storage Area	Description
/pub	Files containing the most recently processed and released data.
/ref	Files containing the most recent reference data.

subject

The subject portion of the naming convention indicates the type of data in the file, such as SADR data, Pharmacy, or Population data. The subject always includes the Data Type but it may also include a Qualifier and Subtype if needed. A Qualifier is used to further describe the Data Type. A Subtype is used to distinguish a particular subset of data from a Data Type. Each element of the subject is described in the sections below.

Data Type

The Data Type is used to indicate the type of data contained in the file. It generally is a recognized data format (e.g., SADR, SIDR), but can also be used to indicate applied processing (e.g., NAGG, PBEN). Data Types that currently exist include those described in Table 3-2.

Table 3-2. Data Types in /mdr/pub

Data Type	Description	Comments
ANCILLARY	Ancillary Data	Contains all ancillary radiology and laboratory records from CHCS
APPT	Appointment Data	
BSURV	Beneficiary Survey Data	
CAPER	Comprehensive Ambulatory/Professional Encounter Record Basic	Source: CHCS / ADS, basic data with no augmentation, more robust than SADR.
CASEMGMT	Case Management	
Death	Casualty, Encounter Death Data, Master Death File	
DEERS	DEERS VM6 Data, VM4 (old), PITE (old)	Includes Detail, ENR, LENR, LVM, Summary
DENTAL	Dental Claims and Provider	Contains both MMSO and ADDP data, separately.
DESPROV	Designate Provider: Clinical, Pharmacy, and Provider	Source System: Iowa Foundation Medical Care file
EAS4	MEPRS data	
HCPR	Health Care Provider Record data	No longer updated. See TEDPR.
HCSRI	HCSR – Institutional data	No longer updated. See TEDI.
HCSRN	HCSR – Non-institutional data	No longer updated. See TEDNI.
MCFAS	Managed Care Forecasting and Analysis System	
MEQS	MEPRS Executive Query System data	No longer updated. See EAS4.
NAGG	Summary level NAS data	
NBEN	Detailed beneficiary-level NAS data	
NMOP	National Mail Order Pharmacy	No longer updated. See PDTS.
PDTS	Pharmacy Data Transaction Service data	
REFERRAL	Referral data	
RESERVIST	Reservist beneficiary data	
SADR	Standard Ambulatory Data Record data	
SIDR	Standard Inpatient Data Record data	
TEDI	Tricare Enrollment Data - Institutional	

Data Type	Description	Comments
TEDNI	Tricare Enrollment Data - Noninstitutional	Two files: CHAMPUS , TDEFIC
TEDPR	Tricare Enrollment Data - Provider	
WWR	Worldwide Workload Report data	Older Micro DMIS data are qualified as WWRDMS.

Data Qualifiers

The Qualifier is an optional item of the subject portion of the naming convention. It is used primarily to indicate a type of legacy data. When present, it is appended to the Data Type. An example using a Qualifier is /mdr/pub/wwrDMS/fy98/wwrDMS.fy98/fy98.sas7bdat, where 'wwrDMS' represents Older Micro DMIS data. Qualifiers identified to date are shown in Table 3-3.

Table 3-3. Data Qualifiers

Qualifier	Description	Comments
DMS	Legacy data produced for the DMIS	
RLP	Legacy data produced by the RLP	

Data Subtype

The subtype is used to distinguish a particular subset of data within a data type. The use and name of a subtype is determined by the entity responsible for creation of the file. An example is /mdr/pub/dental/addp/claims/fy10/fy10.sas7bdat, where 'addp' represents the Active Duty Dental Plan and "claims" indicates that it includes the claims data as submitted by the purchased care dental clinics/providers. The file containing the list of providers is located in /mdr/pub/dental/addp/provider/providers.sas7bdat.

period

The data period portion of the naming convention identifies the file by year and interval (i.e., quarter or month). When this portion of the name and the interval are not present, this indicates that the file is an accumulation of all of the data (e.g., /mdr/pub/sadr/fy10.sas7bdat – a compilation of all the FY10 SADR data available). The meaning of the data period is dependent on the particular data type.

The data period for files in the processed area ('pub') represents the contents of the records contained in the file. For example, DEERS PITE Aggregate data are stored as fyyy, fmmm based on the period of eligibility. The file path and name is therefore /mdr/pub/deers/summary/pagg/fyyy/fmmm/popagg.sas7bdat. The Direct Care SIDR data are stored as fyyy based on the disposition date. The file name is therefore /mdr/pub/sidr/fyyy/sidr.fyyy/fyyy.sas7bdat.

Data Year

The year (/fyyy or /cyyy) portion of the naming convention identifies the calendar or fiscal year of the data. The year will be either cyyy or fyyy for calendar or fiscal, respectively. The basic rule is that data representative of a month should use calendar year (and calendar month). Processed Data representative of other periods longer than a month are stored as fiscal year (and fiscal quarter).

Data Interval

Some data files are annual files, whereas others are quarterly or monthly. The interval portion of the name ([*fqq*] for fiscal quarter; or [*cm^{mm}*] for calendar month) is used only if the file is not an annual file and identifies whether the file contains quarterly or monthly data, as shown in Table 3-4. Note that as the year portion uses Fiscal or Calendar, the interval portion must also use Fiscal Quarter or Calendar Month, respectively. Mixing fiscal and calendar notation between the two fields within a name is not permitted.

Table 3-4. Data Interval Codes

Interval	Description
fq	Fiscal Quarter, used only with fy
cm	Calendar Month, used only with cy

sas_name

A `sas_name` will be needed for all SAS data sets. This name is the member name of the SAS data set. In a number of cases, the `sas_name` will be the same as the period.

file_type

The `file_type` is required for all files as shown in Table 3-5. Data are typically stored as SAS data sets or as text files.

Table 3-5. File Types

File Type	Description
txt	Flat text file
txt.Z	Compressed text file
sas7bdat	SAS dataset
fmt	SAS format file

Section B-4: General Procedures

This section describes the procedures, responsibilities, and data access rights associated with accepting data. Following the procedures described in this section is essential to preserving the integrity of MDR data. These procedures will continue to evolve as exceptions are uncovered in the process. Any proposed changes should be brought to the attention of the DHSS PO.

Accepting Data into the MDR

Regardless of the source, all data must be accompanied by the appropriate metadata.
MDR File Metadata

Data in the MDR is generally accompanied by metadata. These metadata are entered into the MDR File Catalog database.

Table 4-1. Required Metadata for Information Files

Attribute	Description
File Name	Name of the file.
Data Description	A short paragraph about the data and what it is; can include the period of time represented.
Data Source System	The name of the system from which the data originally came, e.g., ADS, CHCS, DEERS.
Source Production Organization	The organization name of the entity that is responsible for the data. For source data this would be the responsible organization for the source data and for processed data this would be the responsible organization for the processed data. Sometimes the party is the same.
Source Production Unit	The unit name of the contractors or personnel assigned to prepare the data. In some cases this may be blank when no particular unit prepares the data.
Data Elements	A list of the data elements (short name and long name) within each record and the record length, e.g., dmsid, char(4), DMIS Identification Code.
Released Date	The date that the data was released for use after quality checking of the data was completed.
Cataloged Date	The date that the data was cataloged in the MDR.
Data Version	The version of the data. (Should be left blank for most files. Some legacy data processing used alpha versioning of the data, e.g., WWR.)
Data completeness	Typically, a short description of which data are and are not included and the period of time represented.
Number of records	The number of records within the file.
Record format	If the records are fixed-length, the length of the records should be stated; otherwise, this field should mention the structure of the record (e.g., "variable-length -delimited").
Software version	The version of software packages used to process or to create the data.
Reference and Input Files	A list of the reference tables and input files used to process or to create the data. The list should provide the Configuration Management information for the file and not just the file name. The prior month's data file name should be included if it is used as an input to the processing.
File History	A description of the history of this particular data file. Any other file names by which the data may have been referenced and items that distinguish the file from previous versions should be mentioned.
Caveats	A description of any issues inherent to the data.
Change Date	The date that the metadata was last edited. The MDR Catalog tool supplies this date.

Section B-5: PUB Data Types

The following sections describe the MDR “public” (PUB) data types, to include a table that illustrates the data file naming convention. As data types are added or changed, this list will be updated.

As a general reference for what is include in each of the data files, frequency of updates, enhancements, processing rules, etc., please see the list of MDR functional specifications at <http://www.tricare.mil/ocfo/bea/mdr.cfm>. The MDR Data Dictionary is also an excellent source of information (http://www.tricare.mil/ocfo/bea/functional_specs.cfm).

ANCILLARY Data Type

Ancillary (ANCILLARY) data are received from CHCS and contain radiology and laboratory data. Data transmissions began with FY05.

ANCILLARY Data File Naming Convention

ANCILLARY data include...	
Output	/mdr/pub/ancillary/fy<yy>/ancillary.fy<yy>/<yy>.sas7bdat

APPT Data Type

Appointment (APPT) data are received from the CHCS Patient Appointment data. Data are processed into Detail and Summary datasets starting with FY02 data.

APPT Data File Naming Convention

APPT data include...	
Output	/mdr/pub/appt/detail/fy<yy>/fy<yy>.sas7bdat /mdr/pub/appt/summary/sum.sas7bdat /mdr/pub/apptwkly/basic/fyXX, where XX=08+

BSURV Data Type

Beneficiary Survey (BSURV) data are no longer submitted to DHSS PO for placement in the MDR. Data submissions stopped with the FY05 survey which was posted in August 2006. There is no specification but the Interface Control Document (ICD) is available on the same website.

BSURV Data File Naming Convention

BSURV data include...	
Output	/mdr/pub/bsurv/hcs<yy>/hcs<yy>**.sas7bdat /mdr/pub/bsurv/hcs<yy>/formats.sas7bdat /mdr/pub/bsurv/ben/final95/formats.sas7bcat /mdr/pub/bsurv/ben/p1995/final/surveyp.sas7bdat

CAPER Data Type

Comprehensive Ambulatory/Professional Encounter Record (CAPER) transmission occurs daily from Ambulatory Data System (ADS) computers to the DHSS Feed Node, where they are batched and submitted weekly for MDR processing. The CAPER data begins with FY03. There are two types of CAPER data: 1) Basic – as it is received from the sites with very basic processing (e.g., removing duplicates) and 2) Enhanced – the Basic data with many additional processes such as grouping, RVU application, cost application, enrollment information, etc.

CAPER Data File Naming Convention

CAPER data include...	
Output	Basic: /mdr/pub/caper/fy<yy>.sas7bdat Enhanced: /mdr/pub/caper/enhanced/fy<yy>.sas7bdat

CASEMGMT Data Type

The Case Management (CASEMGMT) data is prepared from the MDR Standard Ambulatory Data Record (SADR) data.

CASEMGMT Data File Naming Convention

CASEMGMT data include...	
Output	/mdr/pub/casemgmt/cm.sas7bdat

DEATH Data Type

The death data are available from three sources: Casualty, Encounter and a Master File. The casualty data are transferred from the Washington Headquarters Service (WHS) source to the DHSS feed node at OKC.

The master death file is intended to provide users with an accurate list of beneficiaries whose death we have a record for, including casualty deaths for active duty service members. Records from the SIDR, SADR, HCSR-I, and the Casualty Death files comprise this file.

The encounter death file is intended to provide users with an accurate list of beneficiaries whose death we have a record for. Records from the SIDR, SADR, and HCSR-I comprise this file.

DEATH Data File Naming Conventions

DEATH data include...	
Output	/mdr/pub/death/cas/casdeath.sas7bdat /mdr/pub/death/master/mpidth.sas7bdat /mdr/pub/death/enc/encdead.sas7bdat

DEERS Data Type

There are numerous types of data under the DEERS data type: eligibility, enrollment, reservist, etc. They are all listed under this section.

DEERS VM6

VM6 files include beneficiary-level eligibility and enrollment for FY02 and forward as well as summary files. See the PITE Interface Control Document (ICD 1300-7010-03 Approved DEERS VM-6 Extract Mod 1) for more detail.

DEERS VM6 Data File Naming Conventions

DEERS VM6 data include...	
Output	/mdr/pub/deers/summary/vm6agg/fy<yy>/fm<mm>/popagg.sas7bdat /mdr/pub/deers/detail/vm6ben/fy<yy>/fm<mm>.txt.Z /mdr/pub/deers/enr/vm6enr/fy<yy>/fm<mm>.sas7bdat /mdr/pub/deers/lenr/vm6lenr/fy<yy>.sas7bdat /mdr/pub/deers/lvm/lvm6/fy<yy>.txt.Z

DEERS VSAM MDR 2004 (VM4)

VM4 files include beneficiary-level eligibility and enrollment for FY04-FY06 as well as summary files. See the PITE Interface Control Document (ICD 1300-7010-02 DEERS VM-4 Extract) for more detail.

DEERS VM4 Data File Naming Conventions

DEERS VM4 data include...	
Output	/mdr/pub/deers/summary/vm4agg/fy<yy>/fm<mm>/popagg.sas7bdat /mdr/pub/deers/detail/vm4ben/fy<yy>/fm<mm>.txt.Z /mdr/pub/deers/detail/vm4enr/fy<yy>/fm<mm>.sas7bdat /mdr/pub/deers/lenr/vm4lenr/fy<yy>.sas7bdat /mdr/pub/deers/lvm4/fy<yy>.txt.Z

Enrollment (ENR and LENR)

The TRICARE Enrollment (ENR) and Longitudinal Enrollment (LENR) data are created from the National Enrollment Database (NED) of DEERS. Both the ENR and LENR data are processed monthly. The LENR file is created as an iterative process. Each fiscal year file is built with the first month of TRICARE Enrollment data for that year. As each new month of TRICARE Enrollment data are processed and stored, an additional month of enrollment information is added to the file. Previous FYs of data are not refreshed.

ENR / LENR Data File Naming Conventions

ENR / LENR data include...	
Output	ENR: /mdr/pub/deers/enr/enr/fy<yy>/fm<mm>.sas7bdat, FY98-FY04 /mdr/pub/deers/enr/vm4enr/fy<yy>/fm<mm>.sas7bdat, FY04-FY06 /mdr/pub/deers/enr/vm6enr/fy<yy>/fm<mm>.sas7bdat, FY02 forward LENR: /mdr/pub/deers/lenr/lenr/fy<yy>.sas7bdat, FY98-FY03 /mdr/pub/deers/lenr/vm4lenr/fy<yy>.sas7bdat, FY04-FY06 /mdr/pub/deers/lenr/vm6lenr/fy<yy>.sas7bdat, FY03 forward

PITE (PBEN, PAGG, PAGGRLP)

The Point-in-Time Extract (PITE) data were created from the National Enrollment Database (NED) of DEERS but are no longer received as this format (see VM6BEN). The PITE data are stored as two different Data Types:

- PITE Beneficiary-level (PBEN), FY00-FY03
- PITE Aggregate-level (PAGG)

Each month's data feed represents a complete snapshot of population as of a specific date. All months of data are retained in the MDR. Legacy processed data are also available for use (PAGGRLP).

PBEN, PAGG, and PAGGRLP Data File Naming Convention

PBEN data include...	
Output	/mdr/pub/deers/detail/pben/fy<yy>/fm<mm>.txt.Z /mdr/pub/deers/summary/pagg/fy<yy>/fm<mm>/popagg.sas7bdat /mdr/pub/deers/summary/paggrlp/fy<yy>/fm<mm>/popagg.sas7bdat

DEERS Specialty Data

There are numerous files associated with eligibility data but are considered specialty files:

- Medicare C (mdc_c)
- Medicare D (med_d)
- Master Person Index (MPI)
- Special Insured Program (SI)
- Special Insured Tobacco Cessation Program (TBCO)
- Special Insured Weight Loss Program (WGHT)
- Derived Special Insured Program (D_SI)

See the MDR DEERS VM6 specification for more detail.

DEERS Specialty Data File Naming Convention

DEERS Specialty data include...	
Output	/mdr/pub/deers/medicare/mdc_c.sas7bdat /mdr/pub/deers/medicare/mdc_d.sas7bdat /mdr/pub/deers/mpi/mpi.txt.Z /mdr/pub/deers/spechcdp/si.sas7bdat /mdr/pub/deers/spechcdp/tbco.sas7bdat /mdr/pub/deers/spechcdp/wght.sas7bdat /mdr/pub/deers/spechcdp/d_si.sas7bdat

DEERS DMIS System

There are numerous files associated with the eligibility counts from the DMIS Summary system which ended many years ago. The downloads of that information were saved in MDR in the datasets described below.

DEERS DMIS data include...	
Output	/mdr/pub/deers/detail/pbendms, FY93-FY99 /mdr/pub/deers/detail/pbenrlp, FY98-FY00 /mdr/pub/deers/detail/pzipdms, FY89-FY99 /mdr/pub/deers/summary/paggdms, FY82-FY91

DENTAL (ADDP and MMSO) Data Type

Active Duty Dental Plan (ADDP) purchased care claims are received from the ADDP contractor. The ADDP data begins with FY09. There is also a provider file. The MMSO data is no longer being captured for the MDR. The MMSO data is from FY02-FY10 and contains both claims and provider data.

Dental Data File Naming Conventions

DENTAL data include...	
Output	ADDP: /mdr/pub/dental/addp/claims/fy<yy>/fy<yy>.sas7bdat /mdr/pub/dental/addp/provider/providers.sas7bdat MMSO: /mdr/pub/dental/mmso/provider/mmso.provider.txt.Z /mdr/pub/dental/mmso/claims/fy<yy>/fy<yy>.sas7bdat

DESPROV Data Type

The Designated Provider (DESPROV) files consist of Clinical (CLIN) and Pharmacy (PHARM) data which represent all clinical and pharmacy encounters, respectively, for which a record has been received in the MDR. The DESPROV files represent providers who are or have been affiliated with the designated provider program.

Designated Provider Data File Naming Conventions

Designated Provider data include...	
Output	/mdr/pub/desprov/fy<yy>/clin.sas7bdat /mdr/pub/desprov/fy<yy>/pharm.sas7bdat /mdr/pub/desprov/prov/prov.sas7bdat

EASIV / MEQS Data Type

The Medical Expense and Performance Reporting System (MEPRS) data are received from the Expense Assignment System (EAS) and posted to the EAS4 area of the MDR. The MEPRS Executive Query System (MEQS) is a legacy system and is no longer updated.

The first fy<yy> files listed in the table below contain large-scale "summary" data including personnel, workload, and expenses. The ancillary, exp_detail, personnel, and wk_detail datasets listed contain more detailed information.

EAS-IV / MEQS Data File Naming Conventions

EAS4 / MEQS data include...	
Output	EAS4 contains FY01 and forward data: /mdr/pub/eas4/fy<yy>/eas4.fy<yy>/fy<yy>.sas7bdat /mdr/pub/eas4/ancillary/fy<yy>/eas4.ancillary.fy<yy>/fy<yy>.sas7bdat /mdr/pub/eas4/exp_detail/fy<yy>/eas4.exp_detail.fy<yy>/fy<yy>.sas7bdat /mdr/pub/eas4/personnel/fy<yy>/eas4.personnel.fy<yy>/fy<yy>.sas7bdat /mdr/pub/eas4/wk_detail/fy<yy>/eas4.wk_detail.fy<yy>/fy<yy>.sas7bdat MEQS contains FY96-FY01 data: /mdr/pub/meqs/fy<yy>/meqs.fy<yy>/fy<yy>.sas7bdat

HCSRI, HCSRN, and HCPR Data Types

The Purchased Care Data as the Health Care Service Record (HCSR) Institutional, Non-Institutional data, and Health Care Provider Record (HCPR) data came from TMA-Aurora. These data types are no longer updated. See the Purchased Care TED data.

HCSR Data File Naming Conventions

HCSR data include...	
Output	HCSR-I: /mdr/pub/hcsri/fy<yy>/hcsri.fy<yy>.txt HCSR-N: /mdr/pub/hcsrn/fy<yy>/hcsrn.fy<yy>.txt HCPR: /mdr/pub/hcpr/hcpr.sas7bdat

MCFAS Data Type

The Managed Care Forecasting and Analysis System (MCFAS) data are processed yearly and provided to DHSS for inclusion in the MDR.

MCFAS Data File Naming Convention

MCFAS data include...	
Output	/mdr/pub/mcfas/fy<yy>/mcfas.fy<yy>/mcfaspop.sas7bdat

NAGG and NBEN Data Type

Non-Availability Statement (NAS) data are no longer being processed. Previously processed files are still available for use. NAS data are stored as two different data types: NAS Aggregate (NAGG), which is summary data, and NAS Beneficiary (NBEN), which is beneficiary-level data.

NAGG and NBEN Data File Naming Convention

NAS data include...	
Output	/mdr/pub/nagg/fy<yy>/nagg.fy<yy>/nasagg.sas7bdat /mdr/pub/nben/fy<yy>/nben.fy<yy>/nasben.sas7bdat

NMOP Data Type

National Mail Order Pharmacy (NMOP) data are no longer processed as a separate data entity (see the PDTS data for NMOP). Previously processed files are still available for use.

NMOP Data File Naming Convention

NMOP data include...	
Output	/mdr/pub/nmop/fy<yy>/nmop.fy<yy>.txt

PDTS Data Type

Pharmacy Data Transaction Service (PDTS) data are received from the Pharmacoeconomic Center (PEC) and contain records for prescriptions filled in direct care, retail, and mail order. There are two files produced each week: 1) detail – prescription level data, saved as a compressed text file; 2) summary – an aggregate of the detail, not prescription level.

PDTS Data File Naming Conventions

PDTS data include...	
Output	/mdr/pub/pdts/detail/fy<yy>/pdts.detail.fy<yy>.txt.Z /mdr/pub/pdts/summary/fy<yy>/pdts.summary.fy<yy>/sum.sas7bdat

REFERRAL Data Type

Referral data are received from CHCS. The data includes those referrals where an appointment was made; if an appointment was not made, the referral data is not included. It also does not contain referrals made by Purchased Care providers.

Referral Data File Naming Convention

Referral data include...	
Output	/mdr/pub/referral/referral.sas7bdat /mdr/pub/refferal/xwalk.sas7bdat

RESERVIST Data Type

The MDR Reservist file is provided by DMDC (DEERS) and contains a cumulative history of contingency activations for all sponsors activated since September 11, 2001.

Reservist Data File Naming Conventions

Reservist data include...	
Output	/mdr/pub/reservist/reservist.sas7bdat /mdr/pub/reservist/legacyreservist.sas7bdat

SADR Data Type

The Standard Ambulatory Data Record (SADR) transmission occurs daily from Ambulatory Data System (ADS) computers to the DHSS Feed Node, where they are batched and submitted weekly for MDR processing. The SADR data begins with FY98. FY98-FY00 are in fiscal quarter (FQ) files; FY01 forward are in FY files. Completion Factors (COMPFAC) that can be applied to FY99-FY02 SADR are also included.

SADR Data File Naming Conventions

SADR data include...	
Output	FY01 and forward: /mdr/pub/sadr/fy<yy>.sas7bdat FY98-FY00: /mdr/pub/sadr/fy<yy>/sadr.fy<yy>.fq<q>/fy<yy>.sas7bdat COMPFAC: /mdr/pub/sadr/compfac/fy<yy>/sadr.compfac.fy<yy>.txt.Z

SIDR Data Type

The Standard Inpatient Data Record (SIDR) data are received from the CHCS source system to the DHSS feed node at OKC. The SIDR data begins with FY89. Completion Factors (COMPFAC) that can be applied to FY99 and forward SIDR are also included.

SIDR Data File Naming Conventions

SIDR data include...	
Output	/mdr/pub/sidr/fy<yy>/sidr.fy<yy>/fy<yy>.sas7bdat /mdr/pub/sidr/compfac/fy<yy>/sidr.compfac.fy<yy>.txt.Z

TEDI, TEDNI, and TEDPR Data Type

The source system of the TRICARE Encounter Data (TED) Institutional and Non-institutional data is the TMA-Aurora HCSR/TED acceptance system's Net Master Databases or the Purchased Care Data Warehouse Databases. The TED Provider data are created by the TRICARE Managed Care Support Contractor's Fiscal Intermediates and forwarded to the TMA-Aurora Claims Acceptance System. The TMA-Aurora Claims Acceptance System (PEPR) provides the records to the MDR.

TEDI, TEDNI, and TEDPR Data File Naming Conventions

TED data include...	
Output	TED-I: /mdr/pub/tedi/fy<yy>/header.sas7bdat /mdr/pub/tedi/fy<yy>/revenue.sas7bdat TED-NI: /mdr/pub/tedni/fy<yy>/champus.sas7bdat /mdr/pub/tedni/fy<yy>/tdefic.sas7bdat TED-PR: /mdr/pub/tedpr/tedpr.sas7bdat

WWR and WWRDMS Data Types

The Worldwide Workload Report (WWR) data are transmitted monthly from the CHCS to the 3 major Service entities, where they are batched and submitted to the DHSS PO for processing. The WWR contains data for outpatient visits, inpatient visits, admissions, dispositions, and bed days. Note that historic WWR data that was processed using the Legacy system micro DMIS system (FY94-FY98) is stored using the data Qualifier DMS with the Data Type WWR thus creating WWRDMS.

WWR and WWRDMS Data File Naming Conventions

WWR and WWR DMS data include...	
Output	/mdr/pub/wwr/fy<yy>/wwr.fy<yy>/fy<yy>.sas7bdat /mdr/pub/wwrdms/fy<yy>/wwrdms.fy<yy>/fy<yy>.sas7bdat

Section B-6: REF Data Types

The following table describes the MDR reference (REF) data tables to include the general naming convention of the data tables. All files starting with /mdr/ref (e.g., addp.saf.txt.z is located in /mdr/ref/addp.saf.txt.z). As data tables are added or changed, this list will be updated.

Not all reference tables have a specification but if one exists, it will be referenced in the table below. The reference file specifications are posted on <http://www.tricare.mil/ocfo/bea/mdr.cfm>.

MDR Reference Files (/mdr/ref/)

File / Location	Description
addp.saf.txt.z	The Service Area File for the Active Duty Dental Plan processor
admin.fyXX.fmt	The administrative tail used with TED in the Incurred but Not Reported (IBNR) process, XX = 01+
ancillary.bilat.cyXX.fmt	Bilateral CPT codes used to fix the Number of Services issue, XX = 04+
ancillary.bilat.fmt	Use ancillary.bilat.cyXX.fmt
ancillary.costs.fyXX	Units costs applied to the ancillary data to derive full and variable costs, XX = 04+
ancillary.rvu.cyXX	RVU table used to apply RVU values to the ancillary data, XX = 04+
ancillary.transfuse.cyXX.fmt	List of DMISID to where Blood Bank workload is incorrect and therefore removed from the laboratory data, XX = 04+
apc.cyXX.txt	CPT/HCPCS to APC code, weight, etc. mapping used in SADR processing, XX = 05+
apgrep.txt	APG codes and descriptions
appt.cmac.txt	Listing of Direct Care Provider Specialty codes, description, and CMAC category
cad.bpa	Bid Price Adjustment DMISIDs, SAS datasets
cad.bpa.cyXX,cmZZ,txt.z	Bid Price Adjustment DMISIDs in text format, XX = 02-06, ZZ = 01, 04, 07, 10
cad.markets.regXX.txt	Market areas by zip code defined by regional TROs, XX = 02, 06, 09
cad.markets.troX.txt	Market areas by zip code defined by regional TROs, X = n, s, w
cad.omni	Catchment Area Directory, aMMYY.sas7bdat, MM = 01-12, YY = 96+
cad.omni.fyXX	Catchment Area Directory, bpa.sas7bdat, prism.sas7bdat, world.sas7bdat
cad.prism.fyXX.txt.z	PRISM CAD, compressed text, XX = 01+
cad.psa.troX.txt	Zip code to Prime Service Area mapping, X = n, s, w
cad.tpr.cy03.cm06.txt.z	TRICARE Prime Remote, obsolete
caper.apc.cyXX.cqZZ.txt	APC code to weight mapping used in CAPER processing, XX = 06+, ZZ = 01-04
caper.apptctab.fyXX	Workload and costs assigned to the appointment-inferred CAPERs, XX = 09+
caper.chcs.fmt	CHCS Box name to host DMISID mapping used in CAPER processing
caper.costs.fyXX	Full and variable unit costs applied to the CAPER data, XX = 09+
caper.csal.fyXX	Full and variable clinician salary unit costs applied to the CAPER data, XX = 09+
caper.delmap.cyXX.txt	Mapping of old CPT codes to valid codes so grouping can be performed, XX = 09+
caper.facflag.cyXX.txt	SAS code used in processing to set the facility indicator, XX = 04+
caper.minvld.fmt	List of invalid MEPRS codes used in CAPER processing to remove test records
caper.prodline.txt	Mapping of MEPRS code to product line, SAS proc format
caper.revenue.cyXX.txt	Mapping of CPT codes to revenue codes, XX = 09+

File / Location	Description
caper.rvu.cyXX	RVU by CPT/HCPCS used in deriving RVU fields in CAPER, XX = 03+
caper.siteid.fmt	DMISID to CHCS Box name mapping used in CAPER processing
cptref.cyXX.txt	CPT/HCPCS codes and descriptions, XX = 98+
dmisid.index	DMISID information (eg branch of service), SAS datasets
dmisid.index.fyXX.txt	Proc format of DMISID to various description fields, XX = 99+
drgreg.fyXX.txt	DRG codes and descriptions, XX = 98-08
eas4.duty.fyXX	Duty codes and descriptions, XX = 01+, see MDR MEPRS Reference *.doc
eas4.mepr3.fyXX	3 rd -level MEPRS Codes and descriptions, XX = 01+, see MDR MEPRS Reference *.doc
eas4.mepr4.fyXX	4 th -level MEPRS Codes and descriptions, XX = 01+, see MDR MEPRS Reference *.doc
eas4.norms.fyXX	Normative data applied to MEPRS data, XX = 03+
eas4.occ.fyXX	DOD and Service Occupation codes and descriptions, XX = 01+, see MDR MEPRS Reference *.doc
eas4.perscat.fyXX	Personnel codes and descriptions, XX = 01+, see MDR MEPRS Reference *.doc
eas4.skill.fyXX	Personnel skill type and suffix codes and descriptions, XX = 01+, see MDR MEPRS Reference *.doc
enr.norms.fyXX	Normative data applied to the enrollment data, XX = 03-09
hcsrnr.vvu.cyXX.txt	RVU by CPT/HCPCS used in deriving RVU fields in HCSRNR, XX = 98-06
icd9dxref.fyXX.txt	ICD-9 Diagnosis Codes and descriptions, XX = 98+
icd9procref.fyXX.txt	ICD-9 Procedure Codes and descriptions, XX = 98+
msdrgref.fyXX.txt	MS-DRG codes and descriptions, XX = 09+
patcat.fmt	Patient Category to Beneficiary Category proc format
pdts.ncpdp.fmt	Format for translating NCPDP into Treatment DMISID and NPI
pdts.ndccro.fmt	NDC carded for record only format to determine if fill location should be "C" rather than "D"
pdts.ndcdq.csv	NDC quantity correction data for adjusting quantity of drug dispensed
proftails.fyXX.fmt	Professional tails used in Incurred but not Reported (IBNR), XX = 04+
rvu.cyXX	Master RVU file in SAS dataset form, contains all RVUs used in both SADR, CAPER, and TEDNI processing, XX = 03+
rvu.cyXX.txt	Master RVU file in text form, contains all RVUs used in both SADR, CAPER, and TEDNI processing, XX = 03+
sadr.adsinfo.txt	SAS input code no longer used
sadr.apgwgt.fyXX.fmt	APG codes with weights proc format, XX = 03+
sadr.apptctab.fyXX	Workload and costs assigned to the appointment-inferred SADRs, XX = 03+
sadr.costs.fyXX.txt	Full and variable unit costs applied to the SADR data, XX = 99-02
sadr.costs.fyXX	Full and variable unit costs applied to the SADR data, XX = 03+
sadr.cptlist.txt	Obsolete.
sadr.csal.fyXX	Full and variable clinician salary unit costs applied to the SADR data, XX = 03+
sadr.eprice.fyXX.txt	Worldwide average cost for enrollees, XX = 99-02
sadr.eprice.fyXX	Worldwide average cost for enrollees, XX = 03+
sadr.epsal.fyXX	Worldwide average cost of clinician salaries for enrollees, XX = 03+

File / Location	Description
sadr.faczip.fy01.txt	DMISID to zip code, proc format, used with FY01 data only
sadr.fcsts.fyXX.txt	Full unit costs applied to the SADR data, XX = 99-04
sadr.gfcost.fyXX.txt	Global full unit costs applied to the SADR data (used when unit costs are not available), XX = 99-04
sadr.glblcost.fyXX.txt	Global variable unit costs applied to the SADR data (used when unit costs are not available), XX = 99-04
sadr.hpaecva.txt	Count visit algorithm
sadr.mdc.fmt	Diagnosis code to Major Diagnostic Category proc format
sadr.meppar.fy99.txt	DMISID to MEPRS Parent DMISID, proc format, FY99 only
sadr.minvld.fmt	List of invalid MEPRS codes used in SADR processing to remove test records
sadr.mtfreg.fyXX.txt	DMISID to region, proc format, XX = 99, 01
sadr.mtfsvc.fyXX.txt	DMISID to branch of service, proc format, XX = 99, 01
sadr.nprice.fyXX.txt	Worldwide average cost for non-enrollees, XX = 99-02
sadr.nprice.fyXX	Worldwide average cost for non-enrollees, XX = 03+
sadr.npsal.fyXX	Worldwide average cost of clinician salaries for non-enrollees, XX = 03+
sadr.prices.fy01	Worldwide average costs for FY01
sadr.prices.fy99.ebc99pr.txt	Worldwide average costs for Enrollment Based Capitation, FY99
sadr.prices.fy99.ebc99sp.txt	Worldwide average costs for Enrollment Based Capitation, FY99
sadr.prov.txt	Obsolete, no longer used in any processing
sadr.provscal.fyXX.txt	XX = 99-07
sadr.provspc	Obsolete. Assignment of Provider Specialty once used in processing (July 2001)
sadr.rvu.cyXX.txt	RVU table used in SADR processing, text files, XX = 98-01
sadr.rvu.cyXX	RVU table used in SADR processing, SAS datasets, XX = 02+
sadr.sds.fmt	APG codes considered same day surgery, proc format
sadr.tcon.fmt	Obsolete, proc format, Provider specialty to some unknown indicator
sadr.tpc.fyXX.txt	Third Party Collection rates for non-APV, XX = 99-02
sadr.tpcapv.fyXX.txt	Third Party Collection rates for APV, XX = 99-02
sidr.apnd.txt	DMISID to DCWID proc format
sidr.asa.fyXX	Adjusted Standardized Amount, XX = 99+
sidr.costs.fyXX	Full and variable unit costs applied to the SIDR, XX = 99+
sidr.drgsurg	Surgical/medical indicator by DRG
sidr.drgwts.fyXX	DRG weights and thresholds used to compute RWP, XX = 93-08
sidr.glblcost.fy99	Global variable unit costs applied to the SIDR data (used when unit costs are not available), FY99
sidr.msdrgsurg	Surgical/medical indicator by MSDRG
sidr.msdrgwts.fyXX	MSDRG weights and thresholds used to compute RWP, XX = 09+
sidr.norms.fyXX	Normative data applied to SIDR, XX = 02+
sidr.plca.fy99	Full and variable unit costs applied to the SIDR, FY99, obsolete, see sidr.costs.fyXX
sidr.prices.fyXX	Worldwide full cost average by DRG, XX = 99+
sidr.pwp	Professional Weighted Product (PWP) used in cost allocation

File / Location	Description
sidr.pwp.fyXX	PWP, Lab, and Rad weights used in cost allocation, XX = 03+
tedi.pctpdalw.fmt	Percent of Amount Gov't Paid to Allowed Amount by Coverage Category
tedni.rvu.cyXX.fmt	RVU table used in TED-NI processing, proc format, XX = 03+
tedni.rvuspc.txt	Provider Specialty codes with indicator to include in RVU computation
tedpr.provspec.fmt	HIPAA Taxonomy to Provider Specialty proc format
tedpr.state.hcsr2ted.fmt	2 character Country Code to 3 character Country mapping
tedpr.state.ted2hcsr.fmt	3 character Country to 2 character Country Code mapping
usnuic.cyXX.cmZZ.txt.z	Navy DMISID to UIC mapping used in VM6 processing, XX = 04+, ZZ = 01-12
wwr.mstrmtf.fyXX.txt	DMISID to Parent DMISID and Branch of Service mapping, "!" delimited, XX = 00-02

Section B-7: Acronyms and Abbreviations

Acronym / Abbreviation	Description
ADS	Ambulatory Data System
AFMOA	Air Force Medical Operations Agency
ASCII	American Standard Code for Information Interchange
BEA	Business and Economic Analysis
BUMED	Bureau of Medicine (Navy)
CAD	Catchment Area Directory
CHCS	Composite Health Care System
CM	Calendar Month
CY	Calendar Year
DEERS	Defense Enrollment Eligibility Reporting System
DMIS	Defense Medical Information System
DMIS ID	Defense Medical Information System Identification
DMS	Data Qualifier, DMIS
DRG	Diagnosis Related Group
DS	Data Storage
DQ&FP	Data Quality and Functional Proponency
DHCAPE	Defense Health Cost Assessment and Program Evaluation
DHSS	Defense Health Services Systems
ENR	Enrollment
FMT	SAS Format file
FQ	Fiscal Quarter
FY	Fiscal Year
HCPR	Health Care Provider Record
HCSR	Health Care Service Record
HCSRI	Health Care Service Record – Institutional
HCSRN	Health Care Service Record - Non-institutional
HPA&E	Health Programs Analysis & Evaluation
LENR	Longitudinal Enrollment
MCFAS	Managed Care Forecasting and Analysis System
MDR	MHS Data Repository
MEPRS	Medical Expense and Performance Reporting System
MEQS	MEPRS Executive Query System
MMSO	Military Medical Support Office
MHS	Military Health System
MTF	Military Treatment Facility (or Medical Treatment Facility)
NAGG	Aggregate-level NAS
NAS	Nonavailability Statement
NBEN	Beneficiary-level NAS
NMIMC	Naval Medical Information Management Center
NMOP	National Mail Order Pharmacy
PAGG	Aggregate-level PITE data
PASBA	Patient Administration Systems and Biostatistics Activity
PBEN	Beneficiary-level PITE data
PDTL	Detail PITE data
PITE	Point-in-Time Extract
PO	Program Office
PUB	Data Storage Area
REF	Data Storage Area
RLP	Residual Legacy Processor
RM	Resource Management
SADR	Standard Ambulatory Data Record
SAS	Statistical Analysis Programming Language
SIDR	Standard Inpatient Data Record

Acronym / Abbreviation	Description
SP	IBM SP – computer type designator
TED-I	Tricare Enrollment Data - Institutional
TMA	TRICARE Management Activity
TRICARE	Tri-Service Care
TXT	File Type for ASCII flat file
VM4	DEERS VSAM MDR 2004
VM6	DEERS VSAM MDR 2006
WWR	Worldwide Workload Report

Appendix C. Load Leveler and Computing Resource Management

Section C-1. General Information

Load Leveler is a batch job scheduling application developed by IBM. It provides the facility for building, submitting and processing batch jobs within a network of machines. Load Leveler matches the job requirements with the best available machine resources. In a multi-user environment, Load Leveler promotes improved system performance, reduces turnaround time, and provides equitable resource distribution for all users.

Without using Load Leveler, the system runs very efficiently with approximately 2 concurrent SAS jobs. However, experience has shown that the system will “bog down” with many jobs running simultaneously. For example, were 8 jobs contending with each other it may take 24 hours to complete these jobs. If instead only 2 jobs “batched” at a time, they would ALL complete in <16 hours.

Load Leveler permits each machine/node to be configured differently. For example, a node that is utilized only during normal duty hours may be configured via Load Leveler for batch jobs/work during off-work hours, when the utilization for its primary purpose is minimal. Another example is where a node dedicated to another project can be utilized as a Load Leveler compute node with a configuration file that will only accept jobs if the CPU utilization is under 25%.

Section C-2. Summary of Load Leveler Benefits

- Load Leveler is able to summarize system usage on all jobs submitted
- Allows systems/nodes to be loaded to achieve high utilization 24/7 (by using queues to schedule the jobs, and submitting them as compute cycles become available)
- Limits contention problems by limiting the number of concurrent programs running on a single node
- Allows benchmarking for future yield management estimates once a baseline of system operation is set and performance is optimized.

Section C-3. User “Batch” environment using Load Leveler

Users log into the Corporate or Service Node using PuTTY (VPN/SSH). Users create SAS program files by transferring files to the system or by using local text editors on the node. Were special scripts NOT in place, users would then have to write a Load Leveler ‘init’ file “wrapper” similar to JCL on the mainframe to define and schedule their job. In order to simplify this process, special scripts have been developed that make these extra steps transparent to the user. The scripts are designed to automatically detect the user's variables, and simplify job submission. With these scripts in place, the user would simply edit his SAS program, and submit the job by typing at the command line:

```
sas program.sas
```

Section C-4. Load Leveler Details

All nodes available to Load Leveler are called a pool. All of the machines in the “pool” have Load Leveler daemons running on them (these client daemons use minimal system resources <3%). There is one Central Manager for the Load Leveler pool. Unlike the pure client daemons, the Central Manager uses some of the CPU resources of its host (5-8%). Its principal function is to coordinate all Load Leveler activities among the machines in the pool. It maintains status information on all the machines and jobs (usage tracking) and makes decisions on where jobs should be run. The Central Manager is transparent to the user community.

Every Load Leveler job MUST be defined in a job command file. Only after defining a job command file, may a user submit the job for scheduling and execution.

Users can elicit their job status information by using the 'llq' command.

Priorities may be changed using the 'llprio' command. Users may only diminish their assigned priority level. Only DHSS Corporate or Service Node Administrators have the authority to increase the priority of a submitted job beyond its normal assigned priority level.

Section C-5. Load Leveler Internals

Load Leveler's behavior is controlled by installation and configuration options set by the DHSS Corporate or Service Node Administrators. There are two primary configuration files:

LoadL_admin file contains:

- User stanzas – define characteristics and limits at a per user level
- Class stanzas – define class parameters including resource limits, permissions.
- Machine stanzas – define machine characteristics and if the machine is a central manager

LoadL_config file contains global configuration information common to all machines across the pool, such as:

- Job management policies
- Which daemons to run on each machines
- Which job classes are allowed on each machine
- Job limits
- Job accounting parameters
- Number of concurrent jobs allowed

Appendix D. Corporate or Service Node Access and Security Requirements

DHSS Computing Environments Access and Security Requirements

Due to the sensitive nature of data contained within the DHSS COMPUTING ENVIRONMENTS, there are several requirements that must be satisfied before obtaining access to the system.

Requirements:

1. Non-DoD employees only: ADP-II/NACLIC Clearance
2. Civilian personnel and Active Duty Service Members conducting research, non-MHS personnel and/or contractors working for the MHS/DoD: Data Sharing Agreement (DSA) on file with the TRICARE Management Activity (TMA) Privacy and Civil Liberties Office
3. Department of Defense (DoD) Information Assurance (IA) Awareness Certificate on file with the DHSS PEO Access Office
4. DHSS COMPUTING ENVIRONMENTS Account Authorization Request Form on file with the DHSS PEO Program Office
5. Encryption of Sensitive Unclassified Data at Rest on Mobile Computing Devices and Removable Storage Media form (if applicable)

1. Non-DoD employees: ADP-II/NACLIC Clearance

Per DoD regulation 5200.2-R, non-DoD employees requesting access to the DHSS Computing Environments are required to have, or have submitted, a request for clearance, with a scheduled Investigation Scheduled Notice (ISN) regarding an Automated Data Processing Level II (ADP-II/NACLIC), or better, position sensitivity designation. This is to give personnel an interim clearance so they can begin working with the application.

For assistance or direction on applying for an ADP-II clearance, contact your organization's Facility Security Officer (FSO). Forms and related information can be found at the OPM Web Site: <http://www.opm.gov/forms/html/sf.asp>.

2. Civilian personnel and active duty service members conducting research, non-MHS personnel and/or contractors working for the MHS/DoD: Data Sharing Agreement (DSA)

Civilian personnel and active duty service members conducting research and non-MHS personnel and/or contractors working for the MHS/DoD requiring access to DHSS Computing Environments data are required to have a current Data Sharing Agreement (DSA) through their sponsoring organization on file with the TRICARE Management Activity (TMA) Privacy and Civil Liberties Office.

If you do not have a DSA please contact TMA Privacy and Civil Liberties Office at dsa.mail@tma.osd.mil.

3. DoD Information Assurance (IA) Awareness Certificate

DoDD 8570.01 "Information Assurance Training, Certification, and Workforce Management", Certified Current as of April 23, 2007, requires that information system applicant/users complete Information Assurance (IA) Awareness Training on an annual basis. In accordance with this directive, the DHSS PEO Access Office must have a copy of your IA Awareness Certificate on file. Certification must be renewed annually prior to expiration in order to maintain continuous access to the DHSS COMPUTING ENVIRONMENTS.

If you have not completed the DoD IA Awareness in the past year, please take the training and test by clicking DoD IA Awareness (for DoD Personnel) at the following site:

<http://iase.disa.mil/eta>. Either print or download the certificate, sign, and fax it to the DHSS PEO Access Office at 866-551-1249, ATTN: DHSS Access. Only one valid IA Awareness Certificate is required annually, even if you have accounts on multiple DHSS PEO applications/systems.

4. DHSS COMPUTING ENVIRONMENTS Account Authorization Request Form

An DHSS COMPUTING ENVIRONMENTS Account Authorization Request Form (AARF) must be completed, signed, and faxed to the DHSS Program Office, ATTN: DHSS Access, Fax# 866-551-1249. A blank DHSS COMPUTING ENVIRONMENTS AARF and instructions for filling out the form follows after the next section.

5. Encryption of Sensitive Unclassified Data at Rest on Mobile Computing Devices and Removable Storage Media

DoD Policy Memorandum, "Encryption of Sensitive Unclassified Data at Rest on Mobile Computing Devices and Removable Storage Media", July 3, 2007

References:

- (a) DoDI 8500.2, "Information Assurance (IA) Implementation," February 6, 2003
- (b) DoDD 8100.2, "Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG)," April 14, 2004, as supplemented by ASD NII/DoD CIO memorandum, same subject, June 2, 2006
- (c) DoD Policy Memorandum, "Department of Defense Guidance on Protecting Personally Identifiable Information (PII)," August 18, 2006
- (d) DoD Policy Memorandum, "Protection of Sensitive DoD Data at Rest on Portable Computing Devices," April 18, 2006

References (a) through (c) require encryption of various categories of sensitive DoD data at rest under certain circumstances. Reference (d) provides recommendations on means to protect sensitive unclassified information on portable computing devices used within DoD and advises that the suggestions are expected to become policy requirements in the near future. This memorandum from the Department of Defense Chief Information Officer dated July 3, 2007 establishes additional DoD policy for the protection of sensitive unclassified information on mobile computing devices and removable storage media. It applies to all DoD Components and their supporting commercial contactors that process sensitive DoD information.

It is DoD policy that:

- (1) All unclassified DoD data at rest that has not been approved for public release and is stored on mobile computing devices such as laptops and personal digital assistants (PDAs), or removable storage media such as thumb drives and compact discs, shall be treated as sensitive data and encrypted using commercially available encryption technology. Minimally, the cryptography shall be National Institute of Standards and Technology (NIST) Federal Information Processing Standard 140-2 (FIPS 140-2) compliant and a mechanism shall be established to ensure encrypted data can be recovered in the event the primary encryption system fails or to support other mission or regulatory requirements. DoD information that has been approved for public release does not require encryption.
- (2) The requirement to encrypt sensitive unclassified data at rest on mobile computing devices and removable storage media is in addition to the management and access controls for all computing devices specified in references (a) through (c),

Encryption

- A FIPS 140-2 approved file encryption algorithm (i.e., AES, 3DES) must be used for full disk encryption to encrypt data on the remote device. Products that may be utilized include but are not limited to:
 - ❖ PGP – <https://www.pgp.com/products/wholediskencryption/index.html>
 - ❖ GuardianEdge – <http://www.guardianedge.com/products/guardianedge-hard-disk-encryption.php>
- Mobile computing equipment users encrypt all temporary folders (e.g., C:\temp, C:\windows\temp, Temporary Internet Files, etc.) so that any temporary files created by programs are automatically encrypted.

DoD Components shall purchase data at rest encryption products through the DoD Enterprise Software Initiative (ESI). The ESI establishes DoD-wide Enterprise Software Agreements / Blanket Purchase

Agreements that substantially reduce the cost of common-use, commercial off-the-shelf software. Information on encryption products that meet the requirements of this policy may be found in Attachment 2. Other implementation details may be found at <http://www.esi.mil> and at <http://iase.disa.mil>.

Commercial vendors must provide data at rest encryption products for all mobile computing devices used to connect to DHSS products.

Instructions for Filling Out the DHSS Computing Environment AARF:

Section 1. Indicate which system area is being requested.

- **MDR (MHS Data Repository):** Direct access to the MDR is reserved for system administrators, DHSS developers, testers, or processors. Users of the MDR access its data from the SCE Corporate or Service Node.
- **Corporate Node:** workspace environment for users supporting non-Service level program offices requesting access to data stored in the MDR (e.g., TMA Health Affairs, TRO South, TMA Resource Management)
- **Service Node:** workspace environment for users supporting a specific Branch of Service requesting access to data stored in the MDR (e.g., Army OTSG, PASBA, BUMED, AFMOA)

Section 2. Indicate your role in accessing the data. Most requestors will choose "End User."

Section 3. Specify the data to be accessed. Most users will list /mdr/pub and /mdr/ref, the public and reference tables environments of the MDR. With special justification (see Appendix F), users can also request /mdr/apub and /mdr/aref, the archived data of the public and reference table environments.

Section 4. Check the category that applies.

Section 5. Provide information about the requestor. If IP address is dynamic, enter "dynamic" for that information.

Section 6. Indicate whether this is a new request or a change request. If it is a change request, provide MDR User ID as indicated.

Section 7A. Answer questions regarding the DoD IA Training.

Section 7B. Proof of DoD IA Training is required for Managed Care Support Contractors only.

Section 8. All contractors must provide the information requested in this section.

Section 9. Indicate Security clearance level. A minimum of ADP Level II is required.

Section 10. Indicate if mobile computing equipment will be used to access the environment. If yes, complete the Mobile Computing Devices and Removable Storage Media Form which is directly after the AARF.

Section 11. Applicants must read, sign, and attesting to statement provided.

Section 12. Enter applicants name in the space provided and complete information for the requestor's Commander, Supervisor, or Security Officer. The named Commander, Supervisor, or Security Officer must sign and date as indicated.

Section 13. Enter government sponsor's information. The name sponsor must sign and date as indicated.

Corporate and Service Node DHSS Computing Environments Account Authorization Request Form (V. 06/15/2011)

1. Please place an X to specify the system area requested for authorized work related access:			
	MDR		Other (specify):
	Corporate Node		
	Service Node		
2. What is your role in accessing the data requested?			
	End User		
	Other		
3. Please specify the data requested for authorized work related access:			
<i>For MDR and Corporate and Service Nodes, list Dataset names to be accessed (by node) attach sheets if needed:</i>			
<input type="checkbox"/> See attached sheet(s)			
4. Employment Category (Please check the category that applies)			
	Government Employee, Uniformed Service Member, Military, or Civil Service working within/for DoD MHS		
	Contractor working within the DoD Military Health System		
	Government Employee, Uniformed Service Member, Military, or Civil Service working for other agency or directorate not a part of the DoD Military Health System		
	Contractor working for Government Agency, not a part of the DoD Military Health System		
	Other (Please describe):		
5. Applicant/Requestor Information			
Rank/GS Level/Title:			
Name (Last, First, MI):			
Complete Office Mailing Address:			
Sponsoring Organization Name: (Not Project Name)			
If Contractor, Employer Name			
Commercial Telephone Number:			
Email:			
IP Address of Workstation:			
Network Translated IP Address:			
Account Validation PIN:			
Enter a 4 digit numeric PIN that you will use to validate your identity for account administration purposes. This must be the same number as entered when registering in the DHSS WebPortal.			
6. Action			
Check action requested: <input type="checkbox"/> NEW <input type="checkbox"/> CHANGE <input type="checkbox"/> DELETE			
If you have a User ID, please enter it here (If your account has expired, enter your last user ID):			
7A. DoD Information Assurance Awareness Training and Test (All applicants EXCEPT MCSC)			
1. Have you successfully completed the DoD Information Assurance Awareness Training and Test?		<input type="checkbox"/> YES <input type="checkbox"/> NO	
2. Have you signed and faxed the DoD Information Assurance Awareness Certificate to DHSS?		<input type="checkbox"/> YES <input type="checkbox"/> NO	
7B. Proof of Dod Information Assurance Awareness Training (MCSC ONLY)			
1. Is a letter on file with DHSS verifying internal annual IA awareness training requirements?		<input type="checkbox"/> YES <input type="checkbox"/> NO	
8. DSA Information: If you are a Contractor please provide.			
Employer Name:			
Project description requiring this access:			
What is the DSA # that exists for this project?			
Project period of performance:			

9. User ADP/Security Clearance Level (mark appropriate level):		
	ADP II	Notes: 1. A minimum of ADP Level II is required. 2. The use of SECRET is authorized if the requestor's clearance has been active within 2 years of application date.
	ADP I	
	Other (specify): Type: _____ Date: _____	
	If SECRET, provide: Date of Birth: _____	Place of Birth: _____
10. Use of Mobile Computing Equipment.		
<input type="checkbox"/> Mobile computing equipment (Laptop computer, external hard drive, CDs/DVDs, floppy disks, PDA, cell phone, or other movable media) WILL BE USED to connect to this DHSS product. Certification on page 101 MUST BE COMPLETED .		
<input type="checkbox"/> Mobile computing equipment WILL NOT BE USED to connect to this DHSS product.		
11. Applicant Signature (All Applicants/Users must read and sign)		
<p>Some data are protected under the provisions of the Privacy Act of 1974 and the Health Insurance Portability and Accountability Act (HIPAA). The data contains patient and provider identity information and thus requires safeguards from unauthorized access and use. I agree to comply with the Privacy Act of 1974 and HIPAA Privacy and Security Rules and to be responsible for the use of this data to properly safeguard patient and provider identifying data. I accept the responsibility for the information and DoD system to which I am granted access and will not exceed my authorized level of system access. I understand that my access may be revoked or terminated for non-compliance with DoD security policies. I accept responsibility to safeguard the information contained in these systems from unauthorized or inadvertent modification, disclosure, destruction, and use. I understand and accept that my use of the system may be monitored as part of managing the system, protecting against unauthorized access and verifying security problems. By signing below, I am acknowledging that I am only authorized to use DHSS COMPUTING ENVIRONMENTS for my current position/duty and agree to notify the DHSS PEO Access Office and relinquish my account upon departure from my current position/duty or when access is no longer required. All sensitive data will be marked "For Official Use Only. The data contained is for official use only."</p>		
Signature		Date
12. Commander, Supervisor, or Security Officer Certification of Citizenship		
<p>By signing below, I am certifying that _____ (applicant) is a U.S. Citizen and has a mission essential or contract-driven requirement to access the M2, and that the DSA referenced, if any, is applicable. I further acknowledge that substantial criminal penalties, including fines and imprisonment, and/or administrative sanctions may be levied against those who violate the provisions of the Privacy Act of 1974 and/or the Health Insurance Portability and Accountability Act (HIPAA). I will report any change in status, duties, position, or location of the applicant that indicate that the access granted hereunder is no longer required. I shall notify the DHSS PEO Access Office upon departure of this applicant from their current position/duty or when access is no longer required.</p>		
Commander/Supervisor/Security Officer Name		
Title or Position		
Organization, Office, Company		
Office Mailing Address		
Email Address		
Commercial Telephone		
Signature		Date
13. Government Sponsor		
Sponsoring Organization Name		
Commander, Supervisor, Sponsor Name (L, F, MI)		
Title		
Office Mailing Address		
Email Address		
Commercial Telephone		
<p>I certify that the above named applicant requires access to the specified area(s) of the DHSS Computing Environment. I will report any change in status, duties, position, or location of the applicant that indicate that the access granted hereunder is no longer required.</p>		
Government Sponsor Signature:		Date:

**IF MOBILE COMPUTING EQUIPMENT WILL BE USED BY THIS APPLICANT, PAGE 101
MUST BE COMPLETED.**

⊗ --- DO NOT WRITE BELOW THIS BOX --- ⊗

14. DHSS Certification (for DHSS PEO use only)

Form WPValidPIN DoD IA Cert Trng AppSigned CertSigned SponSigned DHSSAccess_____

I certify that DHSS requirements have been validated. Specified access is recommended.

DHSS PEO Approving Authority Name:

Signature:

Date:

Mobile Computing Devices and Removable Storage Media Form

DoD Policy Memorandum, "Encryption of Sensitive Unclassified Data at Rest on Mobile Computing Devices and Removable Storage Media", July 3, 2007.

Per (a) DoDI 8500.2, "Information Assurance (IA) Implementation," February 6, 2003, (b) DoDD 8100.2, "Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG)," April 14, 2004, as supplemented by ASD NII/DoD CIO memorandum, same subject, June 2, 2006, (c) DoD Policy Memorandum, "Department of Defense Guidance on Protecting Personally Identifiable Information PII," August 18, 2006, and (d) DoD Policy Memorandum, "Protection of Sensitive DoD Data at Rest on Portable Computing Devices," April 18, 2006 require that:

- (1) All unclassified DoD data at rest that has not been approved for public release and is stored on mobile computing devices such as laptops and personal digital assistants (PDAs), or removable storage media such as compact discs, shall be treated as sensitive data and encrypted using commercially available encryption technology. Minimally, the cryptography shall be National Institute of Standards and Technology (NIST) Federal Information Processing Standard 140-2 (FIPS 140-2) compliant and a mechanism shall be established to ensure encrypted data can be recovered in the event the primary encryption system fails or to support other mission or regulatory requirements. DoD information that has been approved for public release does not require encryption.
- (2) The requirement to encrypt sensitive unclassified data at rest on mobile computing devices and removable storage media is in addition to the management and access controls for all computing devices specified in references (a) through (c).

Handling and Storage

- During travel, laptops and PDAs must be hand carried and never checked as baggage. If possible, carry diskettes or removable hard drives separate from the laptop.
- If a laptop or PDA is stored in a hotel locker room, it must be kept out of plain view. A laptop or PDA may not be left unattended in a vehicle.

Incident Handling

- In the event of any suspicious activity, breach in security of the remote device, or upon the detection of a virus, Trojan Horse, or malware disconnect from the VPN connection, cease all operation on the device, and report the incident to the DHSS IAM, Mr. Nick Saund, Narinder.Saund@tma.osd.mil, or the DHSS IAO, Mr. Imran Shaw, Imran.Shaw.ctr@tma.osd.mil.

Please identify which mobile computing devices/removable storage media you will be using to access or obtain PHI (protected health information) from this DHSS product: (check all that apply)

<input type="checkbox"/> Laptop	<input type="checkbox"/> External Hard Drive	<input type="checkbox"/> CDs/DVDs	<input type="checkbox"/> Floppy Disks
<input type="checkbox"/> PDA	<input type="checkbox"/> Cell Phone	<input type="checkbox"/> Other	

If other, please describe:

Applicant Certification: I understand the requirement for encryption of sensitive unclassified data at rest (in particular, PHI) on mobile computing devices and removable storage media. I certify that a data at rest encryption product, meeting the DoD specifications has been installed and is operating on any such mobile computing devices that I will use to access data from this DHSS product. Further, I certify that I will ensure that this data at rest encryption product shall be maintained at the most recent version and shall be kept updated according to manufacturers' latest available patches, service packs or other product updates. Further, I will keep this product installed and operational as long as my DHSS product account is active.

Applicant Signature _____ **Date** _____

Applicant Printed Name _____

Information Assurance Manager/Information Assurance Officer Certification: I certify that I have personal knowledge of the installation and proper operation of data at rest encryption product on the above named applicant's computer. I will ensure that required updates are applied as available. Make and model of mobile computing device(s):

Make	Model	Serial Number

IAM/IAO Signature _____ **Date** _____

IAM/IAO Printed Name _____

IAM/IAO email address _____ **0** _____

Phone _____

DD 2875 Form and CAC are required to access Corporate and Service Nodes

Requirements for SCE User Access to DISA DECC Oklahoma City (OKC)

1. All users must meet requirements for and have a DoD issued Common Access Card (CAC) or smartcard.
2. All users must have submitted a DISA Form DD2875, System Authorization Access Request (SAAR), which is available at <http://www.dtic.mil/whs/directives/infomgt/forms/forminfo/forminfo3211.html>. Once you complete the form, print it and obtain required signatures.

The user's Supervisor must complete Part II (blocks 13-25). The user's Facility or Personnel Security Officer must complete Part III (blocks 28-32) regarding security and/or ADP clearance. DISA DECC OKC is the approval authority for this access. Once your account has been approved by DISA, you will receive instructions on how to access the OOB network.

- 2a. On the DD 2875, 3rd box down, where it asks for the "System Name (Platform or Applications)" state:

OKC UNIX OOB Access Account, AIX server account

For users that need Grouper Access, include this as well as the above:

OKC Windows OOB Access Account, Windows Server Account

- 2b. In Box #27, list the server names (node names) and CSHIP names. Items in parentheses should be included for users that need Grouper Access. Most users will need access to either the Corporate or Service Node, depending on what they choose on the DHSS Computing Environment AARF (page 93 for the node descriptions, page 95 for the form). The following information should be listed verbatim in box #27, filling in the highlighted areas with information from the table directly below.

OOB Access to OKC with UNIX (and Windows profiles).
Server account creation on the following AIX (and Windows) servers:
AIX Nxxxx, cship-name UTINIPxx
MDR MCAT N2150: UTINIP26 (rlogin=false, login=true, account_locked=false)
(Windows Wxxxx, cship-nameUTINIxxx)
PIN #####

DHSS System	Node #	CSHIP Name
Corporate Node	2130	UTINIP23
Service Node	2131	UTINIP24
MDR Grouper – Server4	2016w	UTINIX08
MDR Grouper	2018w	UTINIS01

In addition to the information described above, users must also add a 4-digit Personal Identification Number (PIN). It may be the same PIN the user entered on the MDR/SCE AARF. The PIN will be used for authentication purposes when the user calls referencing their account so that identity can be confirmed. The security policy is that if the user cannot recall their PIN correctly, a new DD2875 will need to be submitted to reopen the account.

Example for access to the Service Node, box #27 would contain the following information:

OOB Access to OKC with UNIX
Server account creation on the following AIX servers:
AIX N2131, cship-name UTINIP24
MCAT N2150: UTINIP26 (rlogin=false, login=true, account_locked=false)
PIN = 1234

3. All users must have a DHSS Computing Environment Access Authorization Request Form (CE AARF) on file with the DHSS Access Office. **Persons who have filed within the preceding 12 months do not need to complete a new AARF unless access to the DISA DECC OKC SCE will be made via mobile computing equipment.** There are new requirements for encryption at-rest which must be met by all users of mobile computing equipment. Encryption at-rest software **MUST** be installed on mobile computing equipment and such installation certified. Complete instructions are provided on the CE AARF. See note below for information on mobile computing equipment.
4. All users must obtain (or be provided) a CAC reader and install associated middleware on their workstation or computing equipment. Any reader that handles the DOD issued CAC may be used. Two products tested and known to work are Activeidentity ActivClient CAC Product Version 6.1 (reader part number SCR331) and the SCM Microsystems SCR331. The items are available from a number of suppliers. DHSS does not provide CAC readers to SCE users who are not direct vendors to DHSS.
5. The following chart depicts current SCE user types, current access methods and their corresponding future access methods and requirements.

SCE User Type	Server Type	Current Access Method	Future Access Method	Access Requirements
Inside the MHS VPN Mesh	AIX	Routed through the MHS VPN Mesh	Routed through the MHS VPN Mesh to the Out-of-Band (OOB) Network	<ul style="list-style-type: none"> • 1 – 4 Above • Juniper SSL Client – Instructions will be Provided
On the TMA LAN using GFE	AIX	TMA LAN routed through the MHS VPN Mesh	TMA LAN routed through the MHS VPN Mesh to the OOB Network	<ul style="list-style-type: none"> • 1 – 4 Above • Juniper SSL Client – Instructions will be Provided
On the TMA LAN NOT Using GFE	AIX	TMA LAN routed through the MHS VPN Mesh; When working external to the TMA LAN use Juniper Netscreen VPN Client	TMA LAN routed through the MHS VPN Mesh to the OOB Network; When working external to the TMA LAN use Juniper SSL Client which Connects to the OOB Network	<ul style="list-style-type: none"> • 1 – 4 Above • Juniper SSL Client – Instructions will be Provided
Contractors and Others not captured in the above categories	AIX	Juniper Netscreen VPN Client	Juniper SSL Client which connects to the OOB Network	<ul style="list-style-type: none"> • 1 – 4 Above • Juniper SSL Client – Instructions will be Provided
Users with Access to the Windows Grouper Servers	Windows	Juniper Netscreen VPN Client	Juniper SSL Client which connects to the OOB Network	<ul style="list-style-type: none"> • 1 – 4 Above • Juniper SSL Client – Instructions will be Provided

Encryption of Sensitive Unclassified Data at Rest on Mobile Computing Devices and Removable Storage Media

DoD Policy Memorandum, “Encryption of Sensitive Unclassified Data at Rest on Mobile Computing Devices and Removable Storage Media”, July 3, 2007

References:

(a) DoDI 8500.2, “Information Assurance (IA) Implementation,” February 6. 2003

(b) DoDD 8100.2, "Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG)," April 14, 2004, as supplemented by ASD Nil/DoD CIO memorandum, same subject, June 2, 2006

(c) DoD Policy Memorandum, "Department of Defense Guidance on Protecting Personally Identifiable Information (PII)," August 18, 2006

(d) DoD Policy Memorandum, "Protection of Sensitive DoD Data at Rest on Portable Computing Devices," April 18, 2006

References (a) through (c) require encryption of various categories of sensitive DoD data at rest under certain circumstances. Reference (d) provides recommendations on means to protect sensitive unclassified information on portable computing devices used within DoD and advises that the suggestions are expected to become policy requirements in the near future. This memorandum from the Department of Defense Chief Information Officer dated July 3, 2007 establishes additional DoD policy for the protection of sensitive unclassified information on mobile computing devices and removable storage media. It applies to all DoD Components and their supporting commercial contactors that process sensitive DoD information.

It is DoD policy that:

(1) All unclassified DoD data at rest that has not been approved for public release and is stored on mobile computing devices such as laptops and personal digital assistants (PDAs), or removable storage media such as thumb drives and compact discs, shall be treated as sensitive data and encrypted using commercially available encryption technology. Minimally, the cryptography shall be National Institute of Standards and Technology (NIST) Federal Information Processing Standard 140-2 (FIPS 140-2) compliant and a mechanism shall be established to ensure encrypted data can be recovered in the event the primary encryption system fails or to support other mission or regulatory requirements. DoD information that has been approved for public release does not require encryption.

(2) The requirement to encrypt sensitive unclassified data at rest on mobile computing devices and removable storage media is in addition to the management and access controls for all computing devices specified in references (a) through (c),

Encryption

- A FIPS 140-2 approved file encryption algorithm (i.e., AES, 3DES) must be used for full disk encryption to encrypt data on the remote device. Products that may be utilized include but are not limited to:
 - ❖ PGP: <https://www.pgp.com/products/wholediskencryption/index.html>
 - ❖ GuardianEdge: <http://www.guardianedge.com/products/guardianedge-hard-disk-encryption.php>
- Mobile computing equipment users encrypt all temporary folders (e.g., C:\temp, C:\windows\temp, Temporary Internet Files, etc.) so that any temporary files created by programs are automatically encrypted.

DoD Components shall purchase data at rest encryption products through the DoD Enterprise Software Initiative (ESI). The ESI establishes DoD-wide Enterprise Software Agreements / Blanket Purchase Agreements that substantially reduce the cost of common-use, commercial off-the-shelf software. Information on encryption products that meet the requirements of this policy may be found in Attachment 2. Other implementation details may be found at <http://www.esi.mil> and at <http://iase.disa.mil>.

Commercial vendors must provide data at rest encryption products for all mobile computing devices used to connect to DHSS products.

Both user and organizational information security/assurance certification is required before access is granted where the user will be connecting using a mobile computing device. Completion of this certification is required.

Should you have any questions please contact DHSS Program Office at 703-575-7476.

Please fax the completed form to 1-866-551-1249.

Appendix E. Hierarchical Storage Management (HSM)

Hierarchical Storage Management (HSM)

Tivoli's Hierarchical Storage Management (HSM) software allows users to archive infrequently accessed data to tape storage (freeing up disk space) yet maintain transparent user availability in case the data are required.

HSM File Systems

The Corporate or Service Nodes contains two types of file systems: regular file systems and HSM file systems. A file system is analogous to a drive in the PC world (i.e., C, D).

Regular file systems are made up entirely of disk storage; therefore, all files contained in a regular file system take up space on disk. For instance, if you have 100GB of disk space and make one regular file system, you will get a regular file system that is 100GB in size.

HSM file systems are made up of disk and tape storage. Thus, the total HSM file system size is a result of adding up the size of your available disk and tape space. For example, if you have 100GB of disk, and 900GB of tape, your HSM file system will essentially be 1TB in size.

When a file is placed in a HSM file system, it initially resides on disk space. As the disk space gets used up, older files are migrated to tape. Files can be forced to migrate to tape as well. This can be done by a System Administrator or via a scheduled job.

Migration of a file from disk to tape storage, or vice versa, is transparent to the user. When the user attempts to recall (i.e., read or edit) a file that has been migrated to tape, HSM will respond to the user with a "Tivoli Space Manager is recalling a migrated file" message. When the prompt returns, the file has been moved back to disk space within the HSM file system and is available to the user.

```
[edwn65_sw]:/hsm1/ha > ls -lrt
total 8
-rw-r--r--  1 root   sha      34618 Aug 26 12:12 testfile1

[edwn65_sw]:/hsm1/ha > tail -20 testfile1
ANS9283K Tivoli Space Manager is recalling a migrated file.
```

Using HSM File Systems

Files will reside in a HSM file system because of one of the following three reasons:

1. Automatic migration from regular file systems; or
2. User moves the file to a HSM file system; or
3. User specifically writes the file to a HSM file system.

Automatic Migration from Regular File Systems

Most file systems have a migration rule implemented when the file system is set up by DHCAPE and DHSS personnel. Most migration rules are between 30 and 120 days. The migration rule is negotiable between DHCAPE and the file system authority, within the constraint that there must be a single rule for all files in a file system (i.e., migrate all files within file system 'x' if they have not been used in 'y' days).

User Moves the File to a HSM File System

A user may move a file that exists in a regular file system to HSM space. The directory structure in the HSM file system is exactly the same as the regular file system, with the exception of the /hsm1 prefix.

If a user has a file in /beagov/ called bigfile.txt, the user can move the file into a HSM file system using the mv command:

```
mv source_file_name target_file_name
```

```
e.g., mv /beagov/bigfile.txt /hsm1/beagov/bigfile.txt
```

User Specifically Writes the File to a HSM File System

A user can specifically choose to write his/her file in HSM space. For example, instead of telling SAS (via a filename statement in the program) to save the output file in:

```
/beagov/bigoutput.txt
```

The user should tell SAS to save the output file in:

```
/hsm1/beagov/bigoutput.txt
```

Appendix F. Special Justification Example

MHS DATA REPOSITORY (MDR)
SPECIAL JUSTIFICATION EXAMPLE

Date:

User Name(s) & ID:

Company:

DUA #:

Data Requiring Special Justification:

Justification:

Sponsor Approval:

Printed Name and Title:

Date:

Signature:

DHCAPE Approval:

Printed Name and Title:

Date:

Signature:

DHSS Approval:

Printed Name and Title:

Date:

Signature:

Appendix G. DISA TOOLS

Host Checker

OKC DISA is pushing a mandatory tool Host Checker from their Juniper router to all computers accessing the OOB VPN. Host Checker is the actual tool that will perform a system check on your computer.

The OKC DISA will check the connecting computer for compliance. A message will appear stating that the computer does not meet the minimum requirements to connect to the OKC DISA network.

OKC DISA will then push out the software to make the computer compliant. Initial deployment was scheduled for 21 November 2008, but enforcement of the business rules being enforced will not be until the OOB user community has been provided the policy. DHSS Security indicates that there will be a new Juniper update, MacAfee update, updated Virus definitions, and finally a Host Checker Update.

The following initial documentation was provided by DHSS Security 16 December 2008.

Host Checker Troubleshooting Guide

What is Host Checker?.....	1
HC client side logs.....	1
HC Server side logs.....	2
Reading HC Logs.....	3

What is Host Checker?

Host Checker is a client-side agent that performs endpoint checks on hosts that connect to the IVE. You can invoke Host Checker before displaying an IVE sign-in page to a user and when evaluating a role mapping rule or resource policy.

The IVE may check hosts for endpoint properties using:

The Host Checker implementation of a supported endpoint security application (Windows only) — The Host Checker client-side agent calls the Host Checker integration function of the specified third-party endpoint security product and examines the return value to see if the product is running in accordance with its configured policies

Host Checker integration using a custom DLL (Windows only)—The Host Check Client Interface enables you to integrate a DLL that performs customized client-side checks. You must install this DLL on each client machine.

Attribute checking — On Windows, Macintosh, or Linux, Host Checker looks for the application fingerprints that you specify, including processes or files. On Windows, Host Checker can also checks registry entries.

If the user's computer does not meet any of the Host Checker policy requirements, you can display a remediation page to the user. This custom-made HTML page can contain your specific instructions as well as links to resources to help the user bring his computer into compliance with each Host Checker policy.

HC Client side logs

1. C:\Documents and Settings\\Application Data\Juniper Networks\Host Checker\dsHostChecker.log

 - a. This log file is useful to isolate the problems related to
 - i. Process idle timeout
 - ii. Show remediation/Hide remediation feature
 - iii. Try Again or any action related to Host checker
2. C:\Documents and Settings\\Application Data\Juniper Networks\Host Checker\dsHostCheckerProxy.log

 - a. This log is generated when Pre-auth tunnel feature is used. Useful to determine the issues related to port-forwarding
3. C:\Documents and Settings\ USERNAME>\Application Data\Juniper Networks\EPCheck\EPCheck.log
 - a. This is the most important log file, this log file contains the policy evaluation results, http Send status.

HC Server side logs

1. User access logs: Please collect user access logs for every failed case.
2. Also try to get policy traces for the session. Useful for troubleshooting login issues and role-mapping issues.

Process Checks

1. Check if the process is present in the Task manager
2. Use online tools to compute the checksum's for the process (For Ex Ping.exe on win2k)

File Checks

1. Double check the presence of file and use MD5 checksum
2. Use "SET" command on the dos prompt to determine the environment variables
3. Make sure that environment variables are set using <%Variable%> syntax
4. Wildcards are supported only for leaf node.
 - a. C:**.doc is not valid
 - b. C:\Test*.doc is valid

Registry Checks

5. Wildcards are not supported
6. Only HKEY_CLASSES_ROOT, HKEY_CURRENT_USER, HKEY_LOCAL_MACHINE, HKEY_USERS, HKEY_CURRENT_CONFIG are supported
7. HKEY_DYN_KEY is not supported

Third Party policies

1. Make sure that process idle timeout is relatively large (Especially incase of Sygate Virtual Desktop)
2. If third party (3P) policies are using tunnel definitions, verify the tunnels in the HC admin page after 3P is uploaded
3. If you run into issues related to connectivity, check the following steps:
 - a. Do a netstat -a -n -p tcp and make sure that 0.0.0.0:<port> is not in the listening state Ex: TCP 0.0.0.0:80 0.0.0.0:0 LISTENING TCP 0.0.0.0:443 0.0.0.0:0 LISTENING
 - b. Also make sure that <Loopback IP>:<Port> is not in the listening state
 - c. If you are using XP + SP2 make sure that the hotfix is installed
 - d. Eliminate any Personal firewall related exceptions
 - e. Examine User access logs for IVE connection requests
 - f. Take TCP dump only for issues related to data getting truncated ...etc
4. If customers/vendors complain about connectivity, create a simple tunnel like 127.0.0.1:8000 www.yahoo.com:80 in the manifest file and upload it (Enforce it). Use IE to browse to 127.0.0.1:8000. If this works (if you get to yahoo) then it is something to do with 3P package.

Connection control policy

1. Remember to enforce the policy after choosing the option in admin page
2. This blocks all incoming TCP connection, UDP packets.
3. There is no option to set the exceptions

4. It allows communications to IVE/Proxy server/DNS/WINS/DHCP and Network Connect (NC) adapter
5. Through NC it allows all incoming and outgoing connections

Remediation

1. Make sure that custom instruction checkbox is set, without this remediation will not be shown
2. Check the expression evaluation carefully, default is all AND

Remediate Actions

1. Kill Process: Same as Process checks as far as MD5's and wildcards are concerned.
2. Killing of process is best-effort, in other-words it kills only if the user has access to terminate the process
3. Deleting the files, no wildcards are supported
4. Conditional evaluation of policies. The conditional policy is to evaluate only when the primary policy fails.

Hosts file modification and potential conflicts with JSAM/WTS

1. If the tunnel definitions are specified using hosts file, then we modify the hosts file to create a loopback dynamically
2. To avoid conflicts with JSAM, we start from 127.0.0.3 (outlook 2000 and JSAM is hard-coded to use 127.0.0.1)
3. HC/WTS creates hosts file backup (hosts_juniper.bak) and creates a RunOnce registry entry
4. All the entries are added with Prefix #[HC_Begin] and #[HC_End]
5. When HC is exiting, it clears only the entries that it made during startup
6. If there are no entries from WTS or JSAM then it copies the backup file to the original location and clears the registry.
7. If HC crashes or reboots then Runonce registry takes care of restoring the hosts file.

Reading HC Logs

```
05/20/2005 18:51:23 dsEPChecker.cpp:164 - CdsEPChecker::customFunction():
```

```
*****Start end point checks*****
```

→ This indicates the time at which End point check is started

```
*****
```

```
*****05/20/2005 18:54:53 dsEPChecker.cpp:217 -
```

```
CdsEPChecker::customFunction(): **** Host Checker was ended
```

```
*****
```

```
*****
```

```
*****
```

→ This indicates the time at which Host Checker is about to exit

Host checker could prevent the user from logging to IVE or could kick user out of session if

- Policies fail
- If client is not able to send the status to the server

To isolate the problems look at the logs related to HTTPSend request

05/20/2005 18:51:24 dsEPChecker.cpp:815 - **CdsEPChecker::httpSend:
HttpSendRequest HTTP_OK**

05/20/2005 18:51:24 dsEPChecker.cpp:779 - CdsEPChecker::sendEPCheckStatus():
Check http status...0

05/20/2005 18:51:24 dsEPChecker.cpp:793 - CdsEPChecker::sendEPCheckStatus():
HTTP_OK

- ➔ This indicates that the communication is okay, in case of errors
HttpSendRequests reports WININET error (Look for Proxy configuration at
the browser and general connectivity to isolate the problem)

Logs related to Policies :

05/20/2005 18:51:23 dsEPChecker.cpp:703 - CdsEPChecker::HttpSendStatus():
szPost = policy:policy_4 status:OK

- ➔ The above line says that policy_4 is ok, if it is not ok then policy failed. Look
at the admin configuration for all the rules in the policy and check manually to
make sure that all rules satisfy and look for provider specific error messages
in the log.
 - Ex: 05/03/2005 14:03:13 dsEPChecker.cpp:646 - [CheckAYT() failed]:
policy_2::ping.exe not found
 - Search the log file with file name, process name, registry key, etc... to
get the exact reason for errors.

DISA CAC-Enabled SSL VPN Solution (Frequently Asked Questions)



1.0 GENERAL

1.1 So what is this new SSL VPN solution?

It is a new remote access solution that utilizes the DoD CAC (Common Access Card) for authentication into the OOB (Out-of-Band) and AdminLAN networks.

1.2 I already have remote access to OOB and/or AdminLAN networks, how is this different?

Unlike your current remote access, this new solution uses two factors (something you have and something you know) for authentication which provides a more secure means of remotely accessing the network. In other words, the only real difference between how it is today and how it will be is that it will utilize your CAC for authentication.

1.3 Why are we going to this new solution?

This new solution helps meet the following federal requirements:

- Homeland Security Directive/HSPD-12
- Federal Information Processing Standard (FIPS) 201
- NIST SP 800-78
- Federal Information Processing Standard (FIPS) 140-2
- NSTISSP #11
- JTF-GNO CTO tasking 06-02
- WARNORD 07-37

1.4 What users does this affect?

ALL users who remotely access the OOB or AdminLAN networks.

1.5 Is there any documentation on this new solution?

Yes. The Remote Access Implementation Guide Version 1.0 and Remote Access Implementation Timeline Version 2.0 were e-mailed out on 8/31/2007.

2.0 CAC RELATED

2.1 Who will be required to use their CAC for authentication?

ALL users who remotely access the OOB or AdminLAN networks.

2.2 What if I don't have a CAC?

ALL DoD employees and contractors are already required to have a CAC. If you don't have one, you need to get one.

2.3 What if I can't get a CAC before November 11th?

We will be accepting other secure forms of identification as a temporary solution until you can obtain a CAC.

2.4 Besides a CAC, what other forms of identification will you be accepting?

At this time, the only other alternative to CAC is a soft certificate. Please see your local security office for proper instructions for obtaining a soft certificate or visit <http://iase.disa.mil/pki/eca/index.html> for more information.

2.5 What product is being used to support this?

Juniper SA (Secure Access) 4000-FIPS are strategically located in the DMZs.

3.0 CLIENT SIDE CHANGES

3.1 Do I need to install any software?

Yes.

3.2 What software will I need to install?

If you have administrative privileges on your PC, the appropriate software will automatically be downloaded and installed on your first attempt to login.

If you do not have administrative privileges on your PC, the following software will need to be manually installed on your PC:

- Juniper Installer Service
- Juniper Network Connect
- Juniper Host Checker

3.3 Where do I (or my system administrator) obtain the software?

<https://opr.csd.disa.mil/ssl/ssl.htm>

3.4 Could you briefly explain the software that is being installed on my PC?

- Juniper Installer Service is sometimes referred to as a "helper" file. It assists the system administrator in upgrading the Juniper software to newer versions and also assists in future software deployments (such as Host Checker).

- Juniper Network Connect is the SSL VPN client. For the current SSL VPN users, it is very similar to the Cisco SSL VPN client.

- Juniper Host Checker is a new feature software that does security checks against your PC. Some example capabilities include specific checks on the Operating System, Virus Scanner and Definitions, Firewall, Anti-Spyware Scanner, Running Ports or Protocols, Files, Registry Settings, etc. Juniper's Host Checker is similar to Cisco's NAC (Network Access Control), formerly Cisco Clean Access.

3.5 Are there any other settings that I need to check?

Yes. You must enable the use of TLS 1.0 in your browser. The most common internet browser is Internet Explorer. To enable TLS 1.0 in Internet Explorer, go to Tools > Internet Options > Advanced > Check "Use TLS 1.0". Additionally, if you have administrative privileges and are using the automated method of software download and installation, you will need to have either ActiveX or Java enabled.

3.6 I have administrative privileges, but the software won't automatically download when I try to connect. Is there anything I should check or enable?

The automatic download requires either ActiveX or Java to be enabled.

3.7 ActiveX and Java are disabled on my PC, what do I do?

You will have to follow the manual install process.

4.0 OOB SOLUTION RELATED

4.1 What do I need to do to get an account?

Please visit <https://opr.csd.disa.mil/ssl/ssl.htm> for instructions on gaining access to the OOB network. Basically, you will have to send a digitally signed e-mail to oo ssl@csd.disa.mil with the appropriate information.

4.2 What is the process after I send a digitally signed e-mail?

CCC-MONT and CCC-OKC are constantly checking the e-mail account and appropriate access levels. After security checks are complete, they assign an account in the Juniper SA and then notify you that your access has been granted or denied.

4.3 How long will it take after I send my digitally signed e-mail?

There are a large number of requests due to the quickly approaching November 11th deadline. Both CCCs are doing an excellent job of creating appropriate access. A few hundred accounts have already been created and users are using the new solution. Access is granted on a first come, first server basis. It will take approximately 1-3 days for account creation depending on the size of the queue when your request was sent.

4.4 Will I have to resubmit my DD Form 2875?

No. During the account creation process your existing DD Form 2875 and current OOB ACS access is checked before you are granted access to the new solution. If you have previously only requested IPsec client access, you will be grandfathered into SSL access.

4.5 What is the website that I will need to use after I have an account to remotely access the OOB network?

<https://vpn.csd.disa.mil/oob>

4.6 I currently have multiple profiles. Will I still have multiple profiles with the new solution?

Yes. Whatever access you have today, you will have under the new system.

4.7 How will I know which profile to use?

The Juniper SA uses "Roles" instead of "Profiles". When logging in, you will have to select which Role you wish to enter as.

4.8 When I login to one Role using my first PC and try to login to a separate Role using a second PC, it doesn't let me. Why?

This is a designed security feature of the Juniper SA.

4.9 What if I need to use two Roles at the same time, what am I suppose to do?

At this time, you will have to login to only one Role at a time. We, along with Security, are working on a solution to merge Role setting which would securely allow a single login to access only the resources that you require.

4.10 The devices I'm access on the OOB aren't CAC-enabled, after 11 November 2008, will I still be able to access them?

Yes. This solution is only CAC-enabling the "front door" into the OOB network. You will still use your normal method of logging into your devices. For example, you will present your CAC to login to the OOB network and then telnet, ssh, RPD, etc. to your device and then use that device's authentication server (ACS, AD, etc.) for authentication/authorization purposes. Furthermore, at this time, some servers and devices are not capable of being CAC-enabled (most routers and switches are a prime example of this).

4.11 I don't have an OOB account, do I need to get one?

Only if you require access to the OOB network.

5.0 AdminLAN SOLUTION RELATED

5.1 Do I do the same process (send a digitally signed e-mail) to gain remote access to the AdminLAN network?

No. The AdminLAN solution authenticates users differently than the OOB solution. The AdminLAN solution checks to see if you exist in the AdminLAN AD (Active Directory) system and then checks what Remote Access Group you are assigned to.

5.2 If I don't need to create an account, how will I gain access?

If you already have an AdminLAN account, you will automatically gain access to the AdminLAN solution when it is fully operational (assuming you have the appropriate software installed).

5.3 What is the website that I will need to use to remotely access the OOB network?

<https://vpn.csd.disa.mil/adminlan>

5.4 How will I know when the AdminLAN is fully operational?

An e-mail will go out stating that the AdminLAN is fully operational. This is expected by this weekend to early next week.

5.5 I'm on the AdminLAN, how will I get my software?

The AdminLAN administrators in OGDN will be pushing out the required software.

5.6 I don't have an AdminLAN account, do I need to get one?

Only if you require access to the AdminLAN network.

6.0 OTHER

6.1 What ports and protocols does this new solution use?

TCP port 443.

6.2 I require "special" non-standard access, will my access be removed?

Yes. However, as long as it is brought to our attention, we will do our best to engineer an appropriate solution.

6.3 I require the use of an IPSec VPN client, can I continue to use it?

No. All users will be using the new SSL VPN client. If there is a technical reason why an IPSec VPN client is required, please bring it to our attention so that we can engineer an appropriate solution.

6.4 I can't use the SSL VPN solution. My transfers take too long. What am I supposed to do?

Please document and report what transfers are required to/from what devices and why those transfers are required over the desired network so that we can engineer an appropriate solution.

6.5 I'm at a non-standard AdminLAN site, what do I do?

Each non-standard AdminLAN solution will require a non-standard engineering solution to accommodate. The details (per site) are currently being worked, but any solution will only be temporary. Your local site system administrator will provide the details and migration plan.

6.6 When will Host Checker be implemented?

At this time, the date at which Host Checker will be turned on has not been set. An agreed upon Host Checker Security Policy, basically which checks to perform on who, has not been written.

7.0 EXISTING REMOTE ACCESS TERMINATION

7.1 What is date that the existing remote access solutions will be turned off?

Originally November 11th, 2007 however it has been extended to an undetermined date.

7.2 How will the access be removed?

The Cisco WebVPN module that hosts the current SSL VPN solution will be shutdown and any configurations that allow remote access via an IPSec VPN client will be removed.

Juniper VPN Solution - CAC Enabled Remote Access

A new Juniper SSL VPN solution is being deployed that utilizes the DoD CAC (Common Access Card) for remote access. The new solution supports three separate forms of remote access. One solution is for remotely accessing the OOB Network, one is for remotely accessing the Admin LAN network, and one solution is for remotely accessing non-standard Admin LAN networks.

ALL users will require the use of their CAC to authenticate to each of the solutions.

OOB Users:

- Solution URL: <https://vpn.csd.disa.mil/oob>

Note: If you currently have a requirement to connect to the Out-of-Band (OOB) network you will have to perform the following if you have not yet requested a Juniper OOB Account

- User Requirements: Follow instructions at: <https://opr.csd.disa.mil/ssl/ssl.htm>
- (Basically just send a **digitally signed** e-mail to ostsecurityadmin@okc.disa.mil with appropriate information.)

a) Full Name -

b) Date of Birth -

c) Telephone number -

d) Required profiles –

- Authentication Method: CN (Common Name) of certificate is checked
- Account Creation: CCC enters CN into Juniper SA

Admin LAN Users:

- Solution url: <https://vpn.csd.disa.mil/adminlan>
- User Requirement: None.
- Users will just browse to the URL.
- Authentication Method: EDIPI from e-mail certificate is checked against
- Admin LAN AD (Active Directory) server
- Account Creation: Ogden creates the Admin LAN accounts (as it is today)

Problem Tracking and Resolution:

If you are experiencing difficulty using the new Juniper SSL VPN Solution, please open a ticket with your servicing Operational Support Team (OST).

If you are a customer under the administrative control of the CCC at Oklahoma City, open a ticket with the Oklahoma City OST. You can call the Oklahoma City OST at 405-739-5600 (Commercial), 339-5600 (DSN), or email them at DISAOST@OKC.DISA.MIL.

If you are a customer under the administrative control of the CCC at Montgomery, open a ticket with the Montgomery OST. You can call the Montgomery OST at 334-416-3472 (Commercial), 596-3472 (DSN) or you can email them at MON-DOD OST Ticket Requests@CSD.DISA.MIL.

CCC Oklahoma City manages and maintains network services for SMC Ogden, ISC San Antonio; DECC St. Louis, PE San Diego, PE Rock Island, and PE Dayton.

CCC Montgomery manages and maintains network services for SMC Montgomery, ISC Columbus, Central Staging Chambersburg, BMC Chambersburg, Logistics Chambersburg, PE Jacksonville, PE Warner Robins, PE Norfolk, PE Chambersburg, and PE Huntsville.

Regards,

Corporate Support Team, GS402

DISA, Systems Management Center Ogden

7879 Wardleigh Road Bldg. 891

Hill Air Force Base, Utah. 84056

Com: 801.605.7400 Dsn: 388.7400

CSD@csd.disa.mil