PNNL-16010 Ver. 1.4.6

Federal Emergency Management Information System (FEMIS)

System Administration Guide for FEMIS v1.4.6

JA Arp
JC Bower
RA Burnett
RJ Carter
TR Downing
PM Fangman
LH Gerhardstein
BJ Homer
DM Johnson
RL Johnson
SM Johnson
RM Loveall
TJ Martin
WD Millard
SA Schulze
LR Stoops
S Tzemos
BM Wood

June 25, 1999

Prepared for
the U.S. Department of Energy
under Contract DE-AC06-76RLO 1830

Pacific Northwest National Laboratory
Richland, Washington 99352

DISCLAIMER

Preface

The Federal Emergency Management System (FEMIS) is an emergency management planning and response tool. The following documents were developed to support system users.

This ***FEMIS Data Management Guide*** provides the information needed to manage the data used to support the administrative, user-environment, database management, and operational capabilities of FEMIS.

The ***FEMIS Installation Guide*** provides instructions for installing and configuring the FEMIS software package.

The ***FEMIS System Administration Guide*** provides information on FEMIS System Administrator activities as well as the utilities that are included with FEMIS.

The ***FEMIS Release Notes*** provide a description of what is new in the release, a list of known problems and workaround suggestions, and any information specific to this release that was not available when other documents were published.

The ***FEMIS Bill of Materials*** defines FEMIS hardware, software, and communication requirements.

The ***FEMIS Online Help System*** explains how to use the FEMIS program, which is designed to help civilian emergency management personnel to plan and respond to a Chemical Accident or Incident (CAI) Event at a military chemical stockpile.[1]

---

(1) The FEMIS program is being developed by the Pacific Northwest National Laboratory as part of the U.S. Army Chemical Stockpile Emergency Preparedness Program (CSEPP). Pacific Northwest National Laboratory is operated for the U.S. Department of Energy by Battelle under Contract DE-AC06-76RLO 1830.

Contents

Tables

Figures

Acronyms and Definitions

ACTS	Automated Computer Time Service
ANAD	Name of a FEMIS database (Anniston Depot)
APR	Project file format (ArcView)
CAI	Chemical Accident or Incident
COTS	Commercial-Off-The-Shelf
CPU	Central Processing Unit
CSEPP	Chemical Stockpile Emergency Preparedness Program
CTOO	Name of a FEMIS database (Tooele County)
D2PC	Chemical wind dispersion model used in FEMIS
DAI	Data Acknowledgment Interface
DBMS	Database Management System
DDN	Data Driven Notification
DEI	Data Exchange Interface
DLL	Dynamic Linked Library
DNS	Domain Name Services
DRAM	Dynamic Random Access Memory
E-mail	Electronic Mail
EMIS	Emergency Management Information System
EOC	Emergency Operations Center
ESF	Emergency Support Function
ESIM	Evacuation SIMulation, part of Oak Ridge Evacuation Modeling System (OREMS)
FEMIS	Federal Emergency Management Information System
FTP	File Transfer Protocol
GB	Gigabyte–billion bytes
GID	Group Identification number
GIS	Geographic Information System
GMT	Greenwich Mean Time
GPF	General Protection Fault
GPS	Global Positioning System
GUI	Graphical User Interface
HCL	Hardware Compatibility List
IBS	Integrated Baseline System
ICG	Oracle7 Installation & Configuration Guide Release 7.3.4
IDYNEV	Interactive DYNamic EVacuation
IP	Internet Protocol
KB	Kilobyte–thousand bytes
LAN	Local Area Network
MB	Megabyte–million bytes
Met	Meteorological
MHz	Mega hertz–millions of cycles per second
NFS	Network File System
NIST	National Institute of Standards and Technology

NTP	Network Time Protocol
ODBC	Open Data Base Connectivity
OLE	Object Linking and Embedding
OREMS	Oak Ridge Evacuation Modeling System
PC	Personal Computer
PCI	Peripheral Component Interconnect (Intel)
PID	Process Identification number
PNNL	Pacific Northwest National Laboratory
RAM	Random Access Memory
RER	Remote Evacuee Registration
RDBMS	Relational database management system
SMTP	Simple Mail Transfer Protocol
SQL	Structured Query Language
SQL script	Sequence of SQL statements that perform database operations
TCP/IP	Transmission Control Protocol/Internet Protocol
TEAD	Name of a FEMIS database (Tooele Army Depot)
TNS	Transparent Network Substrate
UDP	User Datagram Protocol
UID	User Identification number
UNIX	Generic name for the Server Operating System
UTM	Universal Transverse Mercator
UTST	Name of a FEMIS database (Utah State)
VB	Microsoft Visual Basic
VGA	Video Graphics Array
WAN	Wide Area Network
WINS	Windows Internet Name Service
Windows NT	Microsoft Network Operating System for Workstations
WinSock	Windows Sockets
WWV	NIST radio station broadcasting continuous time status

1.0 Overview

The Federal Emergency Management Information System (FEMIS©)[a] is an emergency management planning and response tool that was developed by the Pacific Northwest National Laboratory[b] (PNNL) under the direction of the U.S. Army Chemical Biological Defense Command. The ***FEMIS System Administration Guide*** provides information necessary for the system administrator to maintain the FEMIS system.

The FEMIS system is designed for a single Chemical Stockpile Emergency Preparedness Program (CSEPP) site that has multiple Emergency Operations Centers (EOCs). Each EOC has personal computers (PCs) that emergency planners and operations personnel use to do their jobs. These PCs are connected via a local area network (LAN) to servers that provide EOC-wide services. Each EOC is interconnected to other EOCs via a Wide Area Network (WAN).

Thus, FEMIS is an integrated software product that resides on client/server computer architecture. The main body of FEMIS software, referred to as the FEMIS Application Software, resides on the PC client(s) and is directly accessible to emergency management personnel. The remainder of the FEMIS software, referred to as the FEMIS Support Software, resides on the UNIX server. The Support Software provides the communication, data distribution, and notification functionality necessary to operate FEMIS in a networked, client/server environment.

The UNIX server provides an Oracle relational database management system (RDBMS) service, ARC/INFO GIS (optional) capabilities, and basic file management services. PNNL developed utilities that reside on the server include the Notification Service, the Command Service that executes the evacuation model, and AutoRecovery.

This client software includes the FEMIS application, government furnished dispersion and evacuation models, and Commercial-Off-The-Shelf (COTS) software applications such as the ArcView GIS geographic information system, and Microsoft Project.

The FEMIS PC software accesses the site-specific database on the server and returns data to the PC. The user can then add, edit, or delete information; make decisions; displays maps; or use other FEMIS functionality. Information is passed back to the FEMIS database and notifications are made to other FEMIS users.

To operate FEMIS, the Application Software must have access to a site specific FEMIS emergency management database. Data that pertains to an individual EOC's jurisdiction is stored on the EOC's local server. Information that needs to be accessible to all EOCs is automatically distributed by the FEMIS database to the other EOCs at the site.

(a) FEMIS software was copyrighted in 1995 by Battelle Memorial Institute.

(b) Pacific Northwest National Laboratory is operated for the U.S. Department of Energy by Battelle Memorial Institute under Contract DE-AC06-76RLO 1830.

The FEMIS databases have been developed in conjunction with Innovative Emergency Management, Inc. (IEM) and the personnel at each site. The validated database will be provided by Pacific Northwest National Laboratory when FEMIS is installed at your site. Please refer to the FEMIS Data ***FEMIS Database Management Guide*** for further information.

Proper installation of the FEMIS software is crucial to the operations of the emergency management system. Many software elements must be installed on a variety of servers and client workstations. Each must be installed and configured according to specifications for proper interoperability. Please refer to the ***FEMIS Installation Guide*** for further information on installation, including directory structures and other configurations.

1.1 Point of Contact

We encourage you to contact us with suggestions or to ask questions. You can contact us by mail, telephone fax or E-mail:

Pacific Northwest National Laboratory
Ranata L. Johnson
P.O. Box 999, MS K7-28
Richland, WA 99352
Telephone: (509) 375-6311
Fax Number: (509) 375-3641
E-Mail address: ranata.johnson@pnl.gov

1.2 Document Organization

This document is organized into eighteen sections and an appendix, as follows:

Section 1.0 – Overview – discusses the FEMIS software system.

Section 2.0 – FEMIS Monitoring Tools – describes how to use the FEMIS monitoring tools to check the status of database replication and the system.

Section 3.0 – FEMIS Notification Service – describes the FEMIS Notification Service that is used to coordinate new data input.

Section 4.0 – FEMIS Command Server – describes the FEMIS Command Service and how PC users can launch the evacuation model.

Section 5.0 – FEMIS Met Application – describes the FEMIS Met applications and their uses.

Section 6.0 – FEMIS Contact Daemon – discusses the FEMIS contact protocol used in all network communication.

Section 7.0 – FEMIS Data Exchange Interface (DEI) – discusses the FEMIS Data Exchange Interface application, which is used to support the transfer of data from Emergency Management Information System (EMIS) to FEMIS.

Section 8.0 – FEMIS Data Acknowledgment Interface (DAI) – discusses the FEMIS Data Acknowledgment Interface, which is used to acknowledge the receipt of data by the FEMIS program.

Section 9.0 – FEMIS GIS Database – describes the FEMIS geographic information system (GIS) database and the components of the spatial database.

Section 10.0 – FEMIS Oracle Database – describes the FEMIS Oracle database, which includes managing the relational database and replication.

Section 11.0 – FEMIS Evacuation Applications – describes the FEMIS evacuation model interface.

Section 12.0 – Server Network Time Protocol Set Up – describes how to set up and synchronize the server time.

Section 13.0 – Security Measures – describes the security provided with FEMIS.

Section 14.0 – Backup Strategy – discusses the recommended backup strategy for file system and Oracle database backups.

Section 15.0 – FEMIS UNIX Server – discusses the maintenance and troubleshooting for the FEMIS UNIX server.

Section 16.0 – FEMIS PC Utilities – describes the utilities available with the FEMIS application.

Section 17.0 – FEMIS Application Error Messages and Troubleshooting – discusses error messages or problems and the methods to resolve these issues.

1.3 Software Products

FEMIS integrates the following Commercial-Off-The-Shelf (COTS) software products.

Table 1.1. Integrated COTS Software Products

Software Application	Software Company
ArcView GIS	Environmental Systems Research Institute, Inc. (ESRI)
NFS Maestro	Hummingbird Communications Ltd.
Solaris and Solstice NFS Client	Sun Microsystems, Inc.
Microsoft Windows NT Workstation	Microsoft Corporation
Microsoft Project for Windows	Microsoft Corporation

Software Application	Software Company
Oracle	Oracle Corporation
SQL*Net, TCP/IP Adapter, and ODBC Driver	Oracle Corporation

FEMIS integrates the following government-furnished software products.

D2PC (January 1999)	U.S. Army Soldier and Biological Chemical Command (SBCCOM)
PARDOS v3.1 (May 1997)	U.S. Army SBCCOM
Evacuation SIMulation Model (ESIM v2.1f13)	Oak Ridge National Laboratory

The following software products are optional.

ARC/INFO	Environmental Systems Research Institute, Inc.
Corel WordPerfect	Corel Corporation
Microsoft Office	Microsoft Corporation

2.0 FEMIS Monitoring Tools

The FEMIS decision support system uses a networked, client/server architecture that requires the management of multiple servers, LAN and WAN networks, replicated relational databases, and onpost-to-offpost communications. As such, System Administrators must have a suite of tools and utilities at their disposal that will allow them to effectively identify and resolve problems as they arise in the extended FEMIS architecture.

Interruptions in FEMIS services can result from network problems, such as

- unpredicted events, such as power failures resulting in server shutdowns
- critical functions including the Oracle databases may cease to operate
- communication services provided by other servers, such as Met, DEI, or EMIS may not be active.

Distributed processing in FEMIS relies on all EOC servers working properly and the network interconnecting them being reliable. As a result, the system should be monitored regularly to detect any abnormal conditions and avoid problems.

This section describes the tools and utilities provided to assist the FEMIS System Administrator in supporting the extended FEMIS architecture. These tools assist in monitoring the system, notifying the FEMIS System Administrator that a problem exits, and, if applicable, automatic repair of system problems. These tools include the following:

AutoRecovery
A UNIX tool, run as a cron job, that monitors the status of the extended FEMIS system and can intrusively notify the System Administrator when there is a significant problem. Where applicable, AutoRecovery will identify problems that can be automatically fixed and fix them. AutoRecovery will provide both a log and notifications on the status of extended FEMIS architecture.

FEMISMon Watcher (FWATCH.EXE)
A PC application that receives notifications from AutoRecovery and graphically displays the status of key FEMIS system components. FWATCH has triggers that will evoke alarms to notify the System Administrator if AutoRecovery detects a significant problem.

FEMIS Monitor PC (FMONPC.EXE)
A PC application that checks FEMIS database replication and displays a graphic representation of replication status.

Network Monitor (WS_WATCH.EXE)
A PC application that graphically depicts the status of the FEMIS network.

2.1 AutoRecovery

The FEMIS AutoRecovery system is an integrated system that monitors the extended FEMIS architecture, notifies the system administration if significant problems arise, and fixes problems that can be automatically repaired. Figure 2-1 illustrates the flow of the monitoring, notification, and recovery effort.

The AutoRecovery system was developed to reduce the involvement of the FEMIS System Administrator in maintaining the system, aid in the identification of problems when they arise, and keep the system up and operating with fewer interruptions.

With AutoRecovery, the ability to repair and/or restart FEMIS processes has been provided along with increased identification capabilities.

It is recommended that AutoRecovery be installed (see Section 2.6, FEMIS AutoRecovery System Description and Installation, in the ***FEMIS Installation Guide***) on each of the servers in the FEMIS network. When that has been completed, the status of all processes tracked by AutoRecovery is recorded in a log on each of the servers every time AutoRecovery executes. Whenever an anomalous event occurs (e.g., database shuts down, network crashes) a log entry is made and a mail message is sent to all AutoRecovery custodians (for details, see 2.6.2, Logging, and Section 2.6.3, Sending E-mail, in the ***FEMIS Installation Guide***). Included in the mail message, when possible, is AutoRecovery's attempt at fixing the problem. For example, when the database listener goes down, AutoRecovery attempts to restart it. It reports that it tried to restart it and reports whether or not it successfully did so.

2.1.1 AutoRecovery Events/Actions

Every time AutoRecovery is executed (from the crontab) it goes through the following set of events and actions.

1. AutoRecovery monitors the status of the following system processes:

inetd	lockd	lpsched	mounted	hclnfsd
nfsd	rpcbind	sendmail	statd	
syslogd	utmpd		xntpd/ntpd	

2. AutoRecovery reports on the amount of available swap space and disk space when it gets below the accepted (configurable) amount.

3. AutoRecovery determines if there is connectivity to the remote hosts.

4. AutoRecovery monitors the status of the E-mail processes.

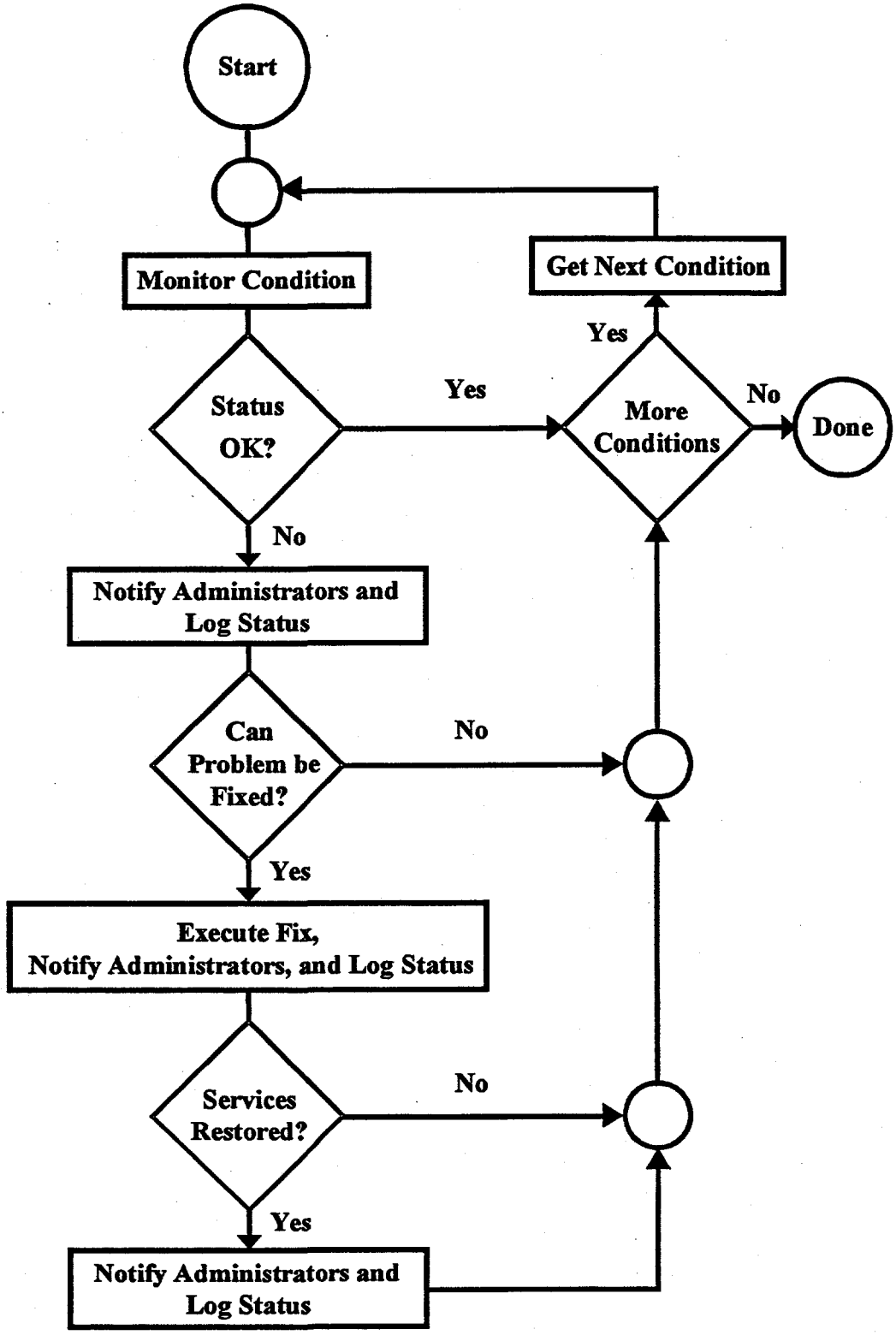


Figure 2.1. AutoRecovery's Integration of Monitoring, Notification, and Recovery

5. AutoRecovery monitors and, by default, attempts to restart the following FEMIS processes:

   femisevent : FEMIS event notification
   femisdei : FEMIS Data Exchange Interface (only if onpost)

6. AutoRecovery monitors the following Oracle Processes and attempts to restart the Oracle Listener (tnslsnr) process when it goes down.

   ora_reco_ ora_smon_ ora_arch
   ora_dbwr_ ora_pmon_ ora_lgwr
   ora_snp_

7. AutoRecovery monitors Oracle's ability to login to the local Oracle database. If successful, it looks for the FEMISDAI, the FEMIS Data Acknowledgment Interface (DAI) job and restarts the DAI, if onpost and not found.

8. AutoRecovery monitors the percentage full for Oracle tablespaces.

9. AutoRecovery monitors and repairs the FEMIS database replication if necessary. It checks on the status of the remote database listeners, remote database connectivity, if fast replication is working, and whether or not there are hung or broken snapshots.

Upon completion of monitoring for all the above events AutoRecovery then:

Logs the results to the femislog file
Mails the results, if warranted, to AutoRecovery custodians
Sends the FEMIS notifications to be picked up by the PC.

2.1.2 Detecting System Problems with AutoRecovery

AutoRecovery attempts to identify and fix, when possible, the root cause of a problem. For example, the AutoRecovery software running onpost identifies that a remote database listener is not running. It notifies the onpost System Administrators of the situation but can not restart the remote listener. Shortly thereafter, it notifies System Administrators that FEMIS replication is broken but does not attempt to fix or restart the Oracle snapshot(s) because the broken snapshot(s) is not the cause of the problem but rather the symptom.

In this case the onpost AutoRecovery will continue to report the broken replication until the remote listener is brought back online (hopefully by the AutoRecovery application running on the remote server), and then it will fix the local snapshot(s).

2.1.3 Using AutoRecovery

The System Administrator can monitor progress of the FEMIS AutoRecovery by monitoring the log file. To monitor progress on the server console, perform the following command: tail -f /var/log/femislog.

A typical (no problems found) report will show a set of messages similar to the following:

```
Jun  9 00:30:02 e.pnl.gov /opt/local/bin/femis_watch: **** Beginning FEMIS Check ****
Jun  9 00:30:02 e.pnl.gov /opt/local/bin/femis_watch: System processes are running
Jun  9 00:30:02 e.pnl.gov /opt/local/bin/femis_watch: Swap space status is okay
Jun  9 00:30:03 e.pnl.gov /opt/local/bin/femis_watch: Disk space status is okay
Jun  9 00:30:03 e.pnl.gov /opt/local/bin/femis_watch: Network connections are reachable
Jun  9 00:30:03 e.pnl.gov /opt/local/bin/femis_watch: email processes are running
Jun  9 00:30:03 e.pnl.gov /opt/local/bin/femis_watch: FEMIS dei processes are running
Jun  9 00:30:03 e.pnl.gov /opt/local/bin/femis_watch: FEMIS event processes are running
Jun  9 00:30:04 e.pnl.gov /opt/local/bin/femis_watch: Oracle processes are running
Jun  9 00:30:05 e.pnl.gov /opt/local/bin/femis_watch: Local listener is up
Jun  9 00:30:06 e.pnl.gov /opt/local/bin/femis_watch: Connected to local Oracle
Jun  9 00:30:06 e.pnl.gov /opt/local/bin/femis_watch: FEMIS dai is running
Jun  9 00:30:07 e.pnl.gov /opt/local/bin/femis_watch: Oracle tablespaces are within limits
Jun  9 00:30:07 e.pnl.gov /opt/local/bin/femis_watch: Fast replication is running
Jun  9 00:30:07 e.pnl.gov /opt/local/bin/femis_watch: Listener fi17 is up
Jun  9 00:30:08 e.pnl.gov /opt/local/bin/femis_watch: Listener fi18 is up
Jun  9 00:30:08 e.pnl.gov /opt/local/bin/femis_watch: Listener fi19 is up
Jun  9 00:30:09 e.pnl.gov /opt/local/bin/femis_watch: Oracle database cgra is available
Jun  9 00:30:10 e.pnl.gov /opt/local/bin/femis_watch: Oracle database cjef is available
Jun  9 00:30:11 e.pnl.gov /opt/local/bin/femis_watch: Oracle database aoes is available
Jun  9 00:30:13 e.pnl.gov /opt/local/bin/femis_watch: Oracle database csal is available
Jun  9 00:30:14 e.pnl.gov /opt/local/bin/femis_watch: Oracle database cpul is available
Jun  9 00:30:15 e.pnl.gov /opt/local/bin/femis_watch: Oracle database cpra is available
Jun  9 00:30:17 e.pnl.gov /opt/local/bin/femis_watch: Oracle database clon is available
Jun  9 00:30:18 e.pnl.gov /opt/local/bin/femis_watch: Oracle database clin is available
Jun  9 00:30:19 e.pnl.gov /opt/local/bin/femis_watch: Oracle database cdal is available
Jun  9 00:30:20 e.pnl.gov /opt/local/bin/femis_watch: Oracle database cclv is available
Jun  9 00:30:21 e.pnl.gov /opt/local/bin/femis_watch: Oracle database cark is available
Jun  9 00:30:22 e.pnl.gov /opt/local/bin/femis_watch: Oracle database mlit is available
Jun  9 00:30:22 e.pnl.gov /opt/local/bin/femis_watch: Oracle database mnlr is available
Jun  9 00:30:23 e.pnl.gov /opt/local/bin/femis_watch: Oracle snapshots are okay
Jun  9 00:30:24 e.pnl.gov /opt/local/bin/femis_watch: FEMIS notification was sent
Jun  9 00:30:24 e.pnl.gov /opt/local/bin/femis_watch: **** FEMIS Check Complete ****
```

When problems are detected the /var/log/femislog file will have error messages similar to the following:

```
Jun  5 15:00:32 e.pnl.gov /opt/local/bin/femis_watch: There are 1 broken snapshots.  The broken
snapshot user id(s) are :  CSAL
Jun  5 15:00:32 e.pnl.gov /opt/local/bin/femis_watch: There are 1 late snapshots.
Jun  5 15:00:32 e.pnl.gov /opt/local/bin/femis_watch: Trying to fix the csal broken snapshot.
Jun  5 15:00:32 e.pnl.gov /opt/local/bin/femis_watch: Snapshot csal was fixed
```

In addition to the /var/log/femislog file the AutoRecovery custodians will receive E-mail. Examples of E-mail messages are as follows:

```
There are 1 broken snapshots. The broken snapshot user id(s) are : CSAL
There are 1 late snapshots.
Trying to fix the csal broken snapshot.
Snapshot csal was fixed
```

AutoRecovery works in conjunction with the PC application FEMISMon Watcher (FWATCH). As AutoRecovery examines that status of the FEMIS architecture, it not only sends messages to the log as described above, it also sends messages to the FEMIS Notification Services. These notifications are picked up by FWATCH. FWATCH will then give a graphical view of the status of key FEMIS components for the site. FWATCH can be set to sound alarms that will intrusively interrupt the administrator or whoever is logged onto the PC where FWATCH is running.

2.1.4 AutoRecovery Error Messages

This section includes AutoRecovery error messages, the problem that caused the error message to display, and possible solutions to resolve the error message.

Table 2.2. AutoRecovery Error Messages

Error Message	Problem	Solution
Cannot connect to local Oracle.	The AutoRecovery system was not able to connect with the local database.	1. Your database administrator should attempt to diagnose why the local database is inaccessible and the exact condition of the database. The database may only be partially shutdown. A complete manual shutdown and startup of Oracle will most likely be required. 2. Check the Oracle tablespace. This message can occur when Oracle is running low on tablespace.
Check for previous femis_watch A previous run of /opt/local/bin/femis_watch did not complete. Please check the following processes: PID COMMAND process id process name	There is another version of AutoRecovery (femis_watch) that has not completed or is hung.	The AutoRecovery message includes a list of processes that are associated with an earlier run of AutoRecovery. Does the list include the Oracle listener process? Has the same process been hung for several cycles of Auto-Recovery? Check the status of the listener (lsnrctl status fi# world). If the status checks out, AutoRecovery should recover on its own. If the listener status does not check out, delete the AutoRecovery

Error Message	Problem	Solution
		processes and check the next iteration of Auto-Recovery for a complete system check.
Connection refused to "servername" port 23.	AutoRecovery could not ping the named server. AutoRecovery will skip all other system and database checks on a system it cannot ping.	1. Your network, router, or server could be experiencing problems. Check with your network or system administrator for the server mentioned in the message. 2. Try the ping –sRv command to check the server for yourself. 3. If you have the traceroute command on your system, use it to track the source of the problem. See the man page on traceroute for more information.
Could not send FEMIS notification.	AutoRecovery has determined that the FEMIS notification daemon is not running.	Check the /var/log/femislog, or the remainder of the E-mail message, to indicate whether or not AutoRecovery was successful in restarting notification. If it was not successful, this could indicate a larger problem. If logging is enabled, check the log files. Double check your FEMIS notification installation/configuration. See Section 3.0, FEMIS Notification Service, for more information. If the problem persists, contact the IEM Help Desk (1-800-939-2737).
Could not status Oracle processes.	At least one of the required Oracle processes is not executing correctly and a review of the Oracle system is recommended.	If this check could not be completed then there is most likely a more serious problem with the database. If there are no other symptoms then your database administrator should diagnose why this database query failed and shutdown and restart Oracle if necessary.
Could not status Oracle tablespaces.	AutoRecovery attempted to measure the amount of data in the Oracle tablespaces but was unable to complete the status check.	If this check could not be completed then there is most likely a more serious problem with the database. If there are no other symptoms then your database administrator should diagnose why this database query failed and shutdown and restart Oracle if necessary.
Database "database user id" is not available.	AutoRecovery could not connect to the remote database.	Notify your database administrator of the remote server of the problem. In most cases this is a known problem

Error Message	Problem	Solution
		and you will be informed of the duration of the outage.
Database "database user id" may not be available.	At least one of the required Oracle processes is not executing correctly and a review of the Oracle system is recommended.	Identify all Oracle processes currently executing on your server. The list should include but is not limited to the following set: PMON, SMON, ARCH, SNP (1 or more is acceptable), LGRW, DBWR, RECO. If any of these processes are missing you may: 1. Have a problem with your operating system that requires a reboot of the server. 2. Have a problem with Oracle that requires a manual shutdown and startup of Oracle. 3. Have an Oracle configuration that does not require the use of the missing processes. In this case you should reconfigure AutoRecovery not to check for the process in the future.
Disk space on "disk" is __% full, __kb used.	The disk space on "disk" has exceeded the threshold configured in /opt/local/bin/femis_watch.conf.	1. The disk threshold is set to 80 by default. You can increase this figure in /opt/local/bin/femis_watch.conf by changing the disk threshold to a higher value. 2. Look for any files or directories that can be deleted. Be on the lookout for any core files that can be deleted. If the disk in question has Oracle export, log or other Oracle files associated with it, check to make sure the Oracle cleanup script is run every week. The cleanup script will not run if the full system backup script fails to complete. If a backup failure is confirmed, rerun the full backup script and delete some of the older oracle export and log files.
Fast replication is not running	Fast replication is not running on the local server.	1. Check with your local database administrator before taking further action. The most likely scenario is

Error Message	Problem	Solution
		that your local database administrator turned fast replication off. 2. If that database administrator cannot provide input into this problem, contact the IEM Help Desk.
FEMIS event is not running on port "port #" Trying to restart FEMIS event.	AutoRecovery has determined that the FEMIS notification daemon is not running.	Check the /var/log/femislog, or the remainder of the E-mail message, to indicate whether or not AutoRecovery was successful in restarting notification. If it was not successful, this could indicate a larger problem. If logging is enabled, check the log files. Double check your FEMIS notification installation/configuration. See Section 3.0, FEMIS Notification Service, for more information on FEMIS Notification. If the problem persists, contact the IEM Help Desk.
FEMIS notification could not be sent.	AutoRecovery has determined that the FEMIS notification daemon is not running.	Check the /var/log/femislog, or the remainder of the E-mail message, to indicate whether or not AutoRecovery was successful in restarting notification. If it was not successful, this could indicate a larger problem. If logging is enabled, check the log files. Double check your FEMIS notification installation/configuration. See Section 3.0, FEMIS Notification Service, for more information. If the problem persists, call the EIM Help Desk.
Local listener is down.	The Oracle listener on the local server has stopped working.	Check the /var/log/femislog or the remainder of the E-mail message to indicate if AutoRecovery was successful in restarting the listener. If the listener was not restarted, check the Oracle alert log for any anomalies and restart the listener (command: lsnrctl start).
Not attempting to fix snapshot "snapshot id".	AutoRecovery did not attempt to fix a broken snapshot because it was not able to identify what needed to be fixed.	This message occurs when the network is not operating correctly. The snapshot cannot be fixed until the network problem has been resolved. Check the status of the network across the site.

Error Message	Problem	Solution
		1. Try the ping –sRv command to check the server for yourself. 2. If you have the traceroute command on your system, use it to track the source of the problem. See the man page on traceroute for more information. If the network is working correctly then your database administrator at the remote EOC should be contacted in order to resolve.
Snapshot "snapshot id" could not be fixed.	AutoRecovery attempted to fix a broken snapshot but was unsuccessful in its attempt.	This message generally occurs when the network or remote server is not operating correctly. Check the status of the network across the site. 1. Try the ping –sRv command to check the server for yourself. 2. If you have the traceroute command on your system, use it to track the source of the problem. See the man page on traceroute for more information. If the network is working correctly, then your database administrator at the remote EOC should be contacted in order to resolve.
Snapshot "snapshot id" was fixed.	This is an acknowledgement that AutoRecovery has successfully fixed a broken snapshot.	This message generally occurs when the network or remote server is not operating correctly. Check the status of the network across the site. 1. Try the ping –sRv command to check the server for yourself. 2. If you have the traceroute command on your system, use it to track the source of the problem. See the man page on traceroute for more information. If the network is working correctly, then your database administrator at the remote EOC should be contacted in order to resolve. Monitor AutoRecovery to verify the problem is resolved.
Stopping snapshot "snapshot id".	AutoRecovery has determined that the network is operational but	Monitor the system and wait for AutoRecovery to execute again to

Error Message	Problem	Solution
	a broken snapshot still exists and cannot be fixed within Oracle. Subsequently, AutoRecovery has attempted to kill the snapshot via its UNIX process id in order for the snapshot to be restarted.	determine if the problem persists.
swap is __% full, __kb used.	Swap space has exceeded the threshold configured in /opt/local/bin/femis_watch.conf.	1. Has the Oracle fixswap cron job run in the last week? Check the oracle crontab for $HOME/admin/dbbackup_cron – fixswap fi#. The line should be uncommented. 2. The swap threshold is set to 80 by default. You can increase this figure in /opt/local/bin/femis_watch.conf by changing swap = 80 to a higher value. 3. Monitor the system. A high value for swap can be a symptom of other problems.
The host "servername" was not statused or is unavailable, skipping listener fi#.	This is a warning that AutoRecovery cannot access the remote server and will skip the remote listener check. You should also see Connect refused to "servername" port 23.	This message generally occurs when the network or remote server is not operating correctly. Check the status of the network across the site. 1. Try the ping –sRv command to check the server for yourself. 2. If you have the traceroute command on your system, use it to track the source of the problem. See the man page on traceroute for more information. If the network is working correctly then your database or system administrator at the remote EOC should be contacted in order to resolve the problem.
The host "servername" was not statused or is unavailable, skipping database "database user name".	This is a warning that AutoRecovery cannot access the remote server and will skip the remote database check. You should also see Connect refused to "servername" port 23.	This message generally occurs when the network or remote server is not operating correctly. Check the status of the network across the site. 1. Try the ping –sRv command to check the server for yourself. 2. If you have the traceroute command on your system, use it to track the source of the problem. See the man page on traceroute for

Error Message	Problem	Solution
		more information. If the network is working correctly then your database administrator at the remote EOC should be contacted in order to resolve the problem.
The tablespace "table space name" is __ % used.	The Oracle table named in the message is outside the threshold defined by AutoRecovery.	1. Increase the Oracle table space. See the System Administration Guide, Section 10.4, How AutoRecovery Works with the Database, for details. 2. Change the threshold for the tablespace in AutoRecovery.
There are __ "daemon name" daemons. The range is set from __ to __.	The number of named daemons is outside the threshold identified by AutoRecovery.	1. Check the rest of the message to see if AutoRecovery corrected the problem. 2. Check the system for other problem associated with the daemon. 3. Change the threshold values for the daemon in /opt/local/bin/femis_watch.conf.
There are 0 femisdei daemons. The range is set from 1 to 1. Trying to restart the femisdei daemon. Restart failed. There are 0 femisdei daemons. The range is set from 1 to 1.	The problem occurred with FEMIS v1.4.5 and is documented here for completness. For some reason, the FEMIS_HOME environment variable is not expanding properly to restart DEI or FEMIS Event.	To resolve this problem edit /opt/local/bin/femis_watch.conf and change the three $ENV{FEMIS_HOME} environment variables on lines 64 and 65 to $ENV{$FEMIS_HOME}.
There are 0 ora_"**"_ daemons. The range is set from ...	The indicated Oracle process is outside the threshold set in AutoRecovery. A review of the Oracle system is recommended.	Identify all Oracle processes currently executing on your server. The list should include but is not limited to the following set: PMON, SMON, ARCH, SNP (1 or more is acceptable), LGRW, DBWR, RECO. If any of these processes are missing you may: 1. Have a problem with your operating system that requires a reboot of the server. 2. Have a problem with Oracle that requires a manual shutdown and startup of Oracle. 3. Have an Oracle configuration that does not require the use of the

Error Message	Problem	Solution
		missing processes. In this case you should reconfigure AutoRecovery not to check for the process in the future. PMON, SMON, ARCH, SNP (1 or more is acceptable), LGRW, DBWR, RECO.
There are 0 tnslsnr daemons. The range is set from 1 to 1. Trying to restart the tnslsnr daemon.	The Oracle listener on the local server has stopped working.	Check the /var/log/femislog or the remainder of the E-mail message to indicate if AutoRecovery was successful in restarting the listener. If the listener was not restarted, check the Oracle alert log for any anomalies and restart the listener (command: lsnrctl start).
There are 2 broken snapshots. The broken snapshot user id(s) are "database user id 1" "database user id 2."	AutoRecovery has found several broken snapshots. This usually indicates a problem with a remote server or network.	Monitor AutoRecovery to see if the problem resolves once the remote server or network is back online.
There are 2 late snapshots.	This is a warning from AutoRecovery indicating that the snapshots have not been refreshed recently.	There is no action required for this message. However, this message is often followed by one of the broken snapshot messages. Monitor subsequent iterations of AutoRecovery for any additional information.
Trying to fix the "snapshot id" broken snapshot.	AutoRecovery has found a broken snapshot and is attempting to fix it.	Check the /var/log/femislog, or the remainder of the E-mail message, to indicate whether or not AutoRecovery was successful in fixing the snapshot. If it was not successful, you will see the message entitled, Snapshot "snapshot id" could not be fixed.
Trying to restart femis dai.	The Data Acknowledgement Interface (DAI) was not working and the AutoRecovery system has attempted to restart it.	Check the /var/log/femislog or the remainder of the E-mail message to indicate if AutoRecovery was successful in restarting the DAI.

2.2 FEMISMon Watcher (FWATCH.EXE)

The FEMISMon Watcher (FWATCH.EXE) program is a PC program that watches for notifications sent by the UNIX AutoRecovery and/or femismon programs. This program shows the status of all the databases, replication snapshots, and other information for each server. It is designed to graphically notify you of a problem. For FWATCH.EXE to provide valid results, femis_event and either AutoRecovery or femismon must be running on the server.

You will only be notified if errors occur.
You can start or stop some of the server programs from your PC using FWATCH. If you click the right mouse button for either a DEI (femisdei) or FEV (femis_event) cell, you will select whether to start or stop the program and enter the password required to execute the command on the window that displays.

It is recommended that you use a password for these functions, and only System Administrators should know these passwords. If no password is needed, leave the password textbox blank. To change the password required for the command, edit the cmdserv.conf file on the server. See the Section 4.0, FEMIS Command Server, for instructions on how to edit this file.

2.2.1 Notification Status

All of the servers for the site are listed across the top of the spreadsheet. The server containing your default EOC will be in uppercase. Down the left of the spreadsheet are all the EOC databases for the site and rows for UNIX server status (SRV), femisdei (DEI) status, and femis_event (FEV) status. The server containing your default EOC will be in uppercase.

As this program gets notifications, it fills in cells on the spreadsheet.

If the item is running correctly, OK is displayed in the cell, and it is colored green.

If the item is not running correctly, the cell is colored either yellow or red (depending on the severity of the error) and contains the text which indicates the error:

ERR:DB – if the database is down
ERR:SNP – if the snapshots are broken
ERR:DEI – if femisdei is not running
ERR:FEV – if femis_event is not running
ERR:SRV – if the server may be down.
ERR:DAI – If the data acknowledgment Oracle job is down.

Clicking on a cell will indicate when the last message for that cell was received and how many minutes ago it was received.

2.2.2 Menu Options

The colors will fade to white as the time since a message was received increases to indicate that the information may be out of date. This feature can be turned on or off using the Fade Colors under Options menu.

As messages are received, the program can beep, flash the window, or display a message to the user. You can choose the notification methods under the Notifications menu. Also under the Notifications menu, you can choose to be notified about messages from all EOCs and servers or just your own EOC and server.

Note: It is highly recommended that you **do not** use the message option for replication errors because many messages may appear if there are replication problems from one server.

If you have indicated that you want to be notified by a flashing window, the window will flash until you click the Stop Flashing menu item under the Options menu.

The Clear Spreadsheet option under the Options menu allows you to blank out the current view.

The Show Messages menu under the Options menu will either show or hide a list box of all the actual messages received from the server.

All the selections for the menu items are stored on the PC in the FEMIS.INI file so they will be the same the next time you start the program.

2.3 FEMIS Monitor PC (FMONPC.EXE)

The FEMIS Monitor PC tool (FMONPC.EXE) checks the FEMIS database replication status and does not require any user privileges to run (does not ask for a user login).

2.3.1 Replication Status

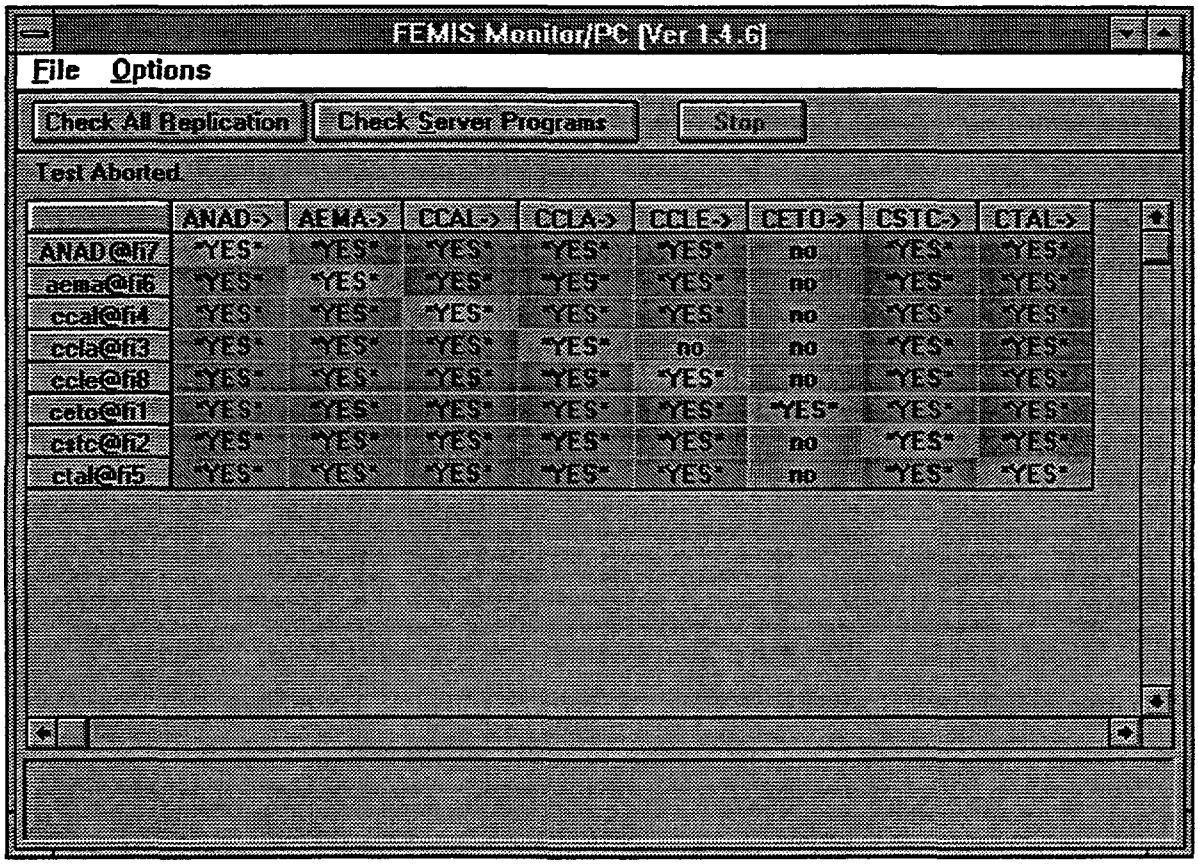
The basic operation is to start the program, then click the Check All Replication button. The program then connects to all databases, writes a record into the REPLICATION_TEST replicated table, and continues to check all the databases to see if the records from the others have been replicated.

A spreadsheet of the results is shown on the FEMIS Monitor/PC window (See Figure 2-2).

- The headers across the top are From Database XXX.
- The headers down the left side are To Database XXX.
- The cells contains the text *YES* if the data has replicated from one database to the other.
- The cells contains the text no if the data has not appeared yet.
- If the program cannot connect to a database, Error is shown for the entire row for that database.
- The spreadsheet should be read Data from database (Column Header) has/has not replicated to database (Row Header).
- Any errors are listed in a scrollable list box at the bottom of the window.

Note: If any of the diagonal items are **no**, then the database **has not** replicated to itself.

Figure 2.2. FEMIS Monitor/PC Window



After each check of all databases, the utility will pause for a number of seconds to reduce its network and server usage. (The number of seconds to pause may be set under the Options menu. The default is 10 seconds.)

This utility will stop checking

1. If all the databases have replicated and everything says *YES*

or

2. If a number of minutes has passed since it started to check. (Under the Options menu, set the number of minutes to keep checking. The default is 10 minutes.)

2.3.2 Options Menu

The following describes menu options.

- Show Replication Timing (approximate) – displays the approximate time it took for the data at one EOC to be replicated to another EOC, instead of putting *YES* in the spreadsheet. To enable this

option, highlight it, and a check mark indicates it has been enabled. Replication times displayed are the times when the data was first found to be replicated at the remote EOC by FMONPC. It is not the time the Oracle database actually performed the replication. If you need a more granular time measurement, configure the Pause between checks option to check at more frequent intervals.

- Stop Checking Replication – sets the length of time to continue checking. Select either 5, 10, or 30 minutes.

- Pause Between Checks – sets the pause length between checks. Select either 5, 10, 20, or 60 seconds.

- Check Replication To and Check Replication From – bring up a list so you can select one row or one column to see if replication is working to or from a single EOC.

- Clear Spreadsheet – clears all entries on the spreadsheet.

- Cleanup All DBs – cleans up the information used by FMONPC in all databases in case there were network, server, database, or PC problems while FMONPC was running.
  Note: Using this option while another PC is running FMONPC can cause items in the spreadsheet to change, such as the whole spreadsheet will change to display no. If no appears from an EOC to itself when YES was previously displayed, then someone else probably used this option.

- Clear Errors – clears the list box of errors at the bottom of the window.

Normally, the monitoring tool is installed only on the System Administrator's PC. It may be installed on a few selected PCs but should not be installed on every PC.

The following example illustrates that most of the database replication is working except that the CETO database has not replicated to any other databases (except itself) and the CCLE database has not replicated to the CCLA database.

2.4 Network Monitor (WS_WATCH.EXE)

The Network Monitor tool graphically shows the network status by coloring icons that indicate the status. This tool should be installed on one PC because it uses network resources when it is running. The PC will periodically send a message (ping) to a set of computers, servers, routers, or other network equipment to see if they respond. The graphical status indicates whether or not the network equipment responded to the ping from this single PC.

Note: The status may not mean that the entire network is up and working correctly, just that some route exists from this PC to the remote equipment. It does not indicate that other points on the network can connect to each other, or that the performance of the network may be unacceptably slow.

Note: To reduce the network resources used, **do not change** the time between checks to less than a minute. Longer durations (e.g., 5, 30, 60 minutes) between checks may be acceptable, depending on the reliability of your network.

Additional information on setting up and configuring the Network Monitor tool (WS_Watch) click on Help on the menu bar.

This tool is freeware and distributed with FEMIS as a useful tool. Any comments or suggestions should be directed to the author of WS_Watch.

3.0 FEMIS Notification Service

3.1 UNIX Host Notification Service

When multiple COTS applications are brought together as in FEMIS, there is the question of how they should work together. The job of the FEMIS application manager is to ensure that all the FEMIS applications can work with one another without user intervention. The inter-task Notification Service is a process for dissimilar applications to communicate with one another during operation. Applications can post and receive event notifications within the FEMIS system with the support of the Notification Service residing on the UNIX host server and on client workstations.

Each workstation hosting the FEMIS client software uses the Notification Service to coordinate activities and data at three levels. The purpose of the Notification Service is to communicate status 1) among active processes on a given workstation; 2) between workstations on the same server; and 3) among workstations on different servers. The Notification Service does not communicate data, but notifies active processes of the availability and location of relevant data in a timely fashion. It is the responsibility of the interested processes to retrieve the data. Likewise, processes, which produce, manipulate, or transform data can notify affected processes of the new state of the data.

The Notification Service also resides on the UNIX host server. Its purpose is to receive and forward notification events to other servers. Workstations connected to this server may emit notification events destined for workstations connected to other servers. These events can be forwarded between servers where the local Notification Service can determine the final destination. The UNIX host server utilizes a relational database for the organization and storage of the enterprise data. The DBMS and any other server process can also use the Notification Service to coordinate activities.

Query, manipulation, and update of data are performed by applications residing in FEMIS workstations. These applications have the responsibility to notify other applications that require the same data of any data changes. This event is communicated via the Notification Service, which serves as the single point of contact that manages the distribution of the event to relevant receivers. When necessary, the Notification Service will propagate the event to distant workstations connected to other servers.

3.1.1 UNIX Notification Service

This section describes the Notification Service residing on the UNIX platform, which serves as the host server. The PC version of the Notification Service is included in the installation of the FEMIS client software. Both versions have identical functions. The UNIX function that implements the Notification Service is called femis_event. The function of femis_event is to provide PC users of the FEMIS event notification system a communication path for the sharing of event information with each other. Events posted at one PC are sent to other PCs on the network by communicating with one or more notification servers.

Local events posted at one PC client workstation are received at the notification server running on LAN, and then sent out to all clients that have expressed an interest in that event.
Global events posted at one PC client workstation are received at the notification server running on LAN, and then sent out to clients on that LAN and also to other notification servers on the WAN.

The femis_event is normally run as a background daemon process. Scripts that are used to startup the FEMIS system also invoke the notification server.

As do all sockets servers, femis_event utilizes a predefined service port on which to listen for client connection requests. By default, the service port is obtained from a definition in /etc/services, the standard UNIX data file of Internet services and aliases. The standard service name of the notification server is femis-notify.

3.1.1.1 Executable Binary Files

Two executable binary files are in the UNIX notification subsystem.

/home/femis/bin/femis_event : notification server executable
/home/femis/bin/fev : a test client for UNIX environment

3.1.1.2 Service Ports Data File

The default service ports for the four FEMIS network protocols are defined in the standard UNIX service ports data file (/etc/services). The IP service port numbers, port names, and descriptions are as follows:

9015	femis-command	command server daemon
9020-29	femis-notify	notification service
9037	femis-metdata	meteorological data daemon
9040	femis-monitor	femis monitor daemon

These four IP service ports must be unique on the host being configured. If for any reason, one or more of these service ports are already in use, then the FEMIS network daemons cannot be successfully initialized and will terminate with a "Port already in use" error. In the event that this happens, contact PNNL immediately, to a reconfigure the IP port addresses, which must be performed before a correct installation of the FEMIS network daemons can be accomplished.

3.1.1.3 Daemon Server Startup

Scripts should be used to start or restart the notification server daemon. The following script will successfully start and restart the command and notification servers:

```
# sh /etc/init.d/femis {start or stop}
```

3.1.2 Notification Server Configuration Options

3.1.2.1 Command-line Options

The command-line options of program femis_event that are defined in this section are

```
femis_event              :  executes in foreground
femis_event -c           : executes a clone in background
femis_event -v           : report the current version
femis_event -V           : report the current + rcs versions
femis_event -q           : quiet mode
femis_event -Q           : really quiet mode
femis_event -d           : executes with many diagnostics
femis_event -a           : enable keep alive mode
femis_event -q -d        : executes with only a few diagnostics
femis_event -L FFFF      : write a verbose log file named FFFF
femis_event -l FFFF      : write a brief log file named FFFF
femis_event -e FFFF      : write an error only log file
femis_event -s SSSS      : specifies service name for getservbyname
femis_event -S           : uses service name femis-notify if found
femis_event -p PPPP      : gets port number from environment variable PPPf
femis_event -t secs      : RESERVED – NOT IMPLEMENTED (see note)
femis_event -i           : report primary ip address and port number
femis_event nnnn         : use port nnnn instead of standard
femis_event host         : connect to named server
femis_event host host    : connect to named servers (see note)
femis_event -r           : use registered service port (1776)
femis_event -conffile    : specify a configuration file path/name
femis_event # host host  : port number # and a list of hosts
femis_event -u           : use unregistered service port (9020-29)
```

Normally, only femis_event -c host will be needed to start executing a notification server. However, the additional options can be mixed to provide logging, diagnostics, and nonstandard service port usage.

3.1.2.2 Clone Process in Background Option

When this option has been included anywhere on the command line, the femis_event program clones itself and then the parent exits, leaving the child process to carry on as a background daemon process.

```
if (fork () != 0)
exit (0);
....
```

Example: femis_event -c

3.1.2.3 Display Version Options

Including -v or -V anywhere on the command line with femis_event, causes the current version or the current version with RCS version to be displayed. Example:

```
% femis_event -v
FEMIS_EVENT - Version 1.0.11 - Wed Dec 14 15:19:49 PST 1994
% femis_event -V
FEMIS_EVENT - Version 1.0.11 - Wed Dec 14 15:19:49 PST 1994
  Copyright © 1994 Battelle Memorial Institute. All Rights Reserved.
RCS: $Id: femis_event.cc,v 1.2 1994/12/14 23:17:08 d31033 Exp d31033$
```

The femis_event version is the current code version, not the FEMIS nor the RCS version. The date and time indicate when the executable was compiled and linked.

3.1.2.4 Diagnostic and Quiet Modes

Using -d causes diagnostics to be printed out when running in foreground mode, i.e., not using option -c. Including -q or -Q with -d limits the amount of diagnostic information printed out. Options -q and -Q mean quiet and real quiet respectively. Using -d alone produces verbose diagnostics. Using -d -q limits the diagnostics. Using -d -Q limits all but severe diagnostics. Examples:

```
% femis_event -q : quiet mode
% femis_event -Q : really quiet mode
% femis_event -d : executes with many diagnostics
% femis_event -q -d : executes with only a few diagnostics
```

3.1.2.5 Service Port Name Option

Including this option lets you specify the service port name on the command line rather than using the default name, femis-notify. Example:

```
% femis_event -c -s evtserv-test-3-eoc
```

For this command to work correctly, the service name evtserv-test-3-eoc must have been entered in the /etc/services data file.

Using option -s causes the standard service port name to be invoked.

3.1.2.6 Service Port Environment Option

This option lets you specify service ports in environment variables. Example:

```
% setenv MY_FEV_PORT 9027
% femis_event -p MY_FEV_PORT -c
```

3.1.2.7 Display IP Address and Service Port

When the notification server is started with the -i option, rather than starting up a Notification Service, it just reports status information about network addresses and then exits. Information displayed includes the date/time of the last build (version identification), name of the local host, primary IP address of the local host, and service port number for the client connections. Example:

```
> su – femis
Password: ********
> femis_event -i
Last build ..... Thu Oct 17 11:54:08 PDT 1996
Host name is ..... fallout.pnl.gov
IP address is ..... 130.20.92.118
Port number is ... 9020
>
```

The purpose of this directive is to obtain information needed in the multiple IP address workaround. Also see Section 2.3.10, Setting Up femis_event, in the ***FEMIS Installation Guide***.

3.1.2.8 Enable Log Files

These options let you enable log file output from femis_event. The -e option creates an errors-only log file. Option -l produces a brief diagnostic log file. Option -L generates a verbose log. Place the desired file name in the argument following -e, -l, or -L. Examples:

```
% femis_event -e errors-only.log.12-24-94 -c
% femis_event -L femis_event.log.12-25-94 -c -p XMAS_PORT
% femis_event -l /home/femis/log/femis_event.log`date +%y%m%d.%H%M`
```

3.1.2.9 Nonstandard Port from Command Line

The notification server can be started with a nonstandard service port without the need for changes in /etc/services (which requires root access) or changing the environment variables simply by including the desired port number on the command line (specify only once). Example:

```
% femis_event -c 9920
% fev - 9920
```

3.1.2.10 Connecting to Other EOC's Notification Server

To have the notification servers at multiple EOCs connected together, include the names of the other EOC server hosts on the command line. Example:

```
server1:% femis_event -c server2
server2:% femis_event -c server1
```

3.1.2.11 Multiple Remote EOC Servers Limitation

For this release, no special server-to-server algorithms for routing had been implemented in the notification server. Smart routing algorithms may be implemented in a future version. Also, the -t option, a part of multi-host, is not implemented.

If you specify only one remote host, you get the optimal routing, which is host-to-host with no alternate conditions or routes.

If you specify two or more remote hosts, the local server connects with all the remote hosts you named. Global event messages are then relayed to all specified remote hosts, even though that may not be necessary. As a result, global messages may be sent to a remote host more than once.

3.1.2.12 Server To Server Connection

The FEMIS UNIX notification server (femis_event) supports a network of multiple notification servers. Any number of server programs can interconnect with each other, and the purpose of this interconnection is to provide a media for communicating global event messages, provided that topology of the network is not a concern.

To establish connection to other servers, a list of notification servers can be included on the command line. The syntax to designate a notification server connection is as follows:

```
host name (uses default service port)
```

In the following lines, all servers use the same default service port number. Example:

```
%femis_event -c countyeoc stateeoc
%femis_event -c irzcountyeoc pazcountyeoc stateeoc
```

Multiple notification servers can be executed on the same host by using a different service port number for each instance. The syntax to designate multiple notification server connections is as follows:

```
%port number>@<host name>
```

In the following lines, two notification servers are started and each is cross connected to the other. Example:

```
%thiseoc:/home/femis/exe/% femis_event -c 9021 9022@thiseoc
%thiseoc:/home/femis/exe/% femis_event -c 9022 9021@thiseoc
```

In the above example, service ports 9021 and 9022 are used rather than the default service port 9020. Server 9021 is connected to server 9022, and server 9022 is connected to server 9021. These connections are on the same host.

In the current FEMIS release, both concepts above have limitations. First, event routing is not optimized for more than two notification servers. Thus, a single event declaration will be sent multiple times on inter-network links.

A network of notification servers can be started by implementing exact topology in a series of startup commands. Example:

```
posteoc% femis_event -c 9020 9020@countyeoc 9020@stateeoc
countyeoc% femis_event -c 9020 9020@posteoc 9020@stateeoc
stateeoc% femis_event -c 9020 9020@posteoc 9020@countyeoc
```

The above example starts notification servers on three hosts: posteoc, countyeoc, and stateeoc. Each is capable of sending global event messages to the other two. No regard is given to topology, i.e., each server sends events to the other two servers, even if having one of the others do a relay would accommodate more efficient use of network bandwidth.

An alternate way to start the servers is to start one, then add one to the network, and later add the third. Example:

```
posteoc% femis_event -c 9020
```

The above established a single notification server. Next enter:

```
countyeoc% femis_event -c 9020 9020@posteoc
```

We now have a two-node event server network: countyeoc connects to posteoc, which learns of the new server–to–server connection. We now have a two-node event server network. Next enter:

```
stateeoc% femis_event -c 9020 9020@posteoc 9020@countyeoc
```

We now have a three-node event server network. Stateeoc connects to both posteoc and countyeoc and each learn of the new server node.

Graceful removal of nodes from the notification server topology and optimization of topology for saving network bandwidth have not yet been implemented. These will be done in future FEMIS releases.

3.1.2.13 Which Service Port to Use

Which service port the notification server uses is determined as follows: from the following list, the first service port that produces a valid service port number is used as the service port method for this daemon server.

- If the port number is included on the command line, then that port is used even if the methods below also produce a valid service port number. Example:

  femis_event 9975

- If a service name is included on the command line (via -s or -S), then that service name is used in a getservbyname() call. If that service name returns a valid service port from the /etc/services data file, then that port is used. Example:

  femis_event -s FEMIS_ShellServer

- If an environment name is included on the command line, then that environment name is translated into a service port number. Example:

  setenv MYPORT 7120 ; femis_event -p MYPORT

- The default service name, femis-notify, is tried in a call to getservbyname(). If that returns a valid service port, then that port number is used.

- The default environment name FEMIS_EVENT_PORT is translated. If that name is defined and translates to a valid port number, then that service port is used.

- If all the above fail, femis_event terminates with an error.

Normally, you can just use the standard service port number from the /etc/services file. However, for testing and diagnostics, additional methods have been included for running additional notification server modules that use a nonstandard port number, so there is no interference with normal operations.

3.1.2.14 Enable Keep Alive

If the UNIX notification server is started with -a specified, keep alive mode for all socket calls is utilized.

3.1.2.15 Registered Service Port

Command line option -r specifies use of the registered service port only. Command line option -u specifies use of the unregistered service ports only. The default starting is registered service port. Previously the default was to unregistered ports. For more information, see Section 6.0, FEMIS Contact Daemon.

3.1.3 femis_event EVENT Configuration File

The femis_event uses a configuration file. This file is located at /home/femis/etc/femis_event.conf. This configuration file contains set up information and details of command line options for auxiliary processes.

femis_event auxiliary processes are utilized by the FEMIS Data Driven Notification (DDN) and DEI. To specify a configuration file path/name other than the default, use the -conf <file> command line option to femis_event.

The configuration file is a text file. Parsing rules are as follows:

Any line starting with a # is a comment line.

The line com port=registered specifies the registered service port to be used. Command line option overrides this command.

The line com port=unregistered specifies the unregistered service port to be used. Command line option overrides this command.

The line com fevpath=femisbin specifies to look in /home/femis/bin for the fev executable.

The line com fevpath=dotslash specifies to look in ./ for the fev executable.

A line starting with aux specifies information pertaining to running auxiliary processes.

Aux argname=on turns argument naming on. In this mode, arguments to the auxiliary process are passed as -<name> <value>. If aux argname=off is specified, arguments are passed just as <value> with no argument naming utilized.

Aux keypos=ITEM specifies the position of which item to key on. Possible ITEMs are msgname, exerid, auxprocessident, and parm#.

Aux ifport=PORT specifies only utilize this command if the notification server's port/protocol is equal to PORT. PORT is a decimal number value.

Aux notport=PORT specifies only utilize this command if the notification server's port/protocol is not equal to PORT. PORT is a decimal number value.

Aux exe=path/file specifies the path/file name of the auxiliary process executable. The file must be tagged as X (executable) in the file system.

Aux key=VALUE specifies what value the key must be in order to select this command.

Aux arg=ITEM specifies an item to include in the argument list to the auxiliary process. The possible ITEM names are msgname, exerid, auxprocessid, parm#, origin, msgflags, message, home, host, port, stdport, and fev.

ITEMs are as follows: MsgName is message name from <...message...>. ExerID is the exercise identification from <...message...>. AuxProcessID is the auxiliary process identification from <...message...>. Parm# is parameter number # from <...message...>. Origin is the complete origin

string from <...message...>. MsgFlags is the message flags from <...message...>. Message is the complete message string <...message...>. Home is the femis_event home directory, e.g., /files13/home/femis. Host is the server's host name. Port is the port/protocol number, e.g., 9020. StdPort is Yes or No depending on whether standard service port (1776) is in affect. fev is the complete string to use for invoking fev, including path, name, and port number.

3.1.4 Notification Server Utilities

3.1.4.1 UNIX Test Client – fev

The notification server subsystem includes a test client for the UNIX system environment. The UNIX client can be used to test features of the command server, both new and old, and to perform certain diagnostics.

Note: This client is not an integral FEMIS system component.

The file name of the test client is fev. The UNIX test client is installed at the same subdirectory as the notification server (see Section 3.1.1.1, Executable Binary Files).

3.1.4.2 UNIX Test Client Command-line Options

Valid command-line options for fev have the same format and usage as the notification server. Example:

```
% fev host nnnn # nonstandard port and host from command
% fev - nnnn # nonstandard port local host (testing only)
% fev -p PPPP # nonstandard port from environment variable
% fev -s SSSS # nonstandard port from /etc/services file
% fev -S # use standard service name femis-notify
% fev -i IDNUM # specify notification client id number
% fev -x # don't exit on eof from standard-input
% fev -u # use unregistered service port (9020-29)
% fev -f: connect to femis_event using FIFO for diagnotstic use
% fev -d: diagnostics enabled
% fev -H: HOMEDIR set path of /home/femis
```

See descriptions of these options in Section 3.1.2, Notification Server Configuration Options.

3.1.4.3 Client ID Number

You can simulate what happens when a notification system client crashes and then comes back online. In that case, the PC/client needs to receive the same client ID number that was assigned to that PC during the previous session. The notification server handles that scenario correctly, but during testing on a single

development host, you need to tell the test client which client is connecting by specifying the client ID from the previous session (see o command reply).

Syntax: fev -i IDNUM

3.1.4.4 Test Client Protocol

To run the notification server test client, do the following:

```
% set path = (/home/femis/exe $path)
% fev # connect to local host, standard port
% fev <remote host> # connect to a remote host
% fev - <port> # connect to nonstandard port on this host
% fev <remote host> <port># connect to nonstandard port on remote host
```

The notification server test client provides several shorthand commands to the actual notification server protocol, as follows:

```
o : sends open-link message (NS_MT_OPENLINK)
: reply message contains the client's link id
c : sends close-link message (NS_MT_CLOSELINK)
i EEEE : sends register-interest message (NS_MT_REGISTER_INTEREST)
r EEEE : sends remove-interest message (NS_MT_REMOVE_INTEREST)
e EEEE : sends declare-event message (NS_MT_EVENTMSG) (nonglobal)
g EEEE : sends declare-global message (NS_MT_EVENTMSG & NS_EF_GLOBAL)
t1 : bombard server with multiple NS_MT_EVENT testing
t2 : bombard server with multiple NS_MT_EVENT testing
```

3.1.4.5 Test Client Example

Example:

```
server1:% femis_event -c 9920 server2
FEMIS_EVENT port is 9020
server2:% femis_event -c 9920 server1
FEMIS_EVENT port is 9020
server3:$ fev server1 9920
FEMIS_EVENT port is 9020
o
<<<<<< received OPENLINK-reply: client-id = 2
l TestEvent
l GlobalEvent
```

```
server4:>%fev server1 9920
FEMIS_EVENT port is 9020
o
<<<<<< received OPENLINK-reply: ...
client-id = 3
e TestEvent

<<<<<< received notification: event=TestEvent

c
^D
server4:% fev server2 9920
o
<<<<<< received OPEN-LINK-reply: ...
client-id = 2
e TestEvent
g GlobalEvent

<<<<<< received notification: event=GlobalEvent

c
^D
c
^D
```

In the example, the operator runs the notification server on two hosts, server1 and server2; they connect to and communicate with each other because the other's host name is on the command line.

Next, the client is run on server3, connecting to server1, a link is opened, and interest is declared in two events, TestEvent and GlobalEvent. Also, the client is run on server4, connecting to server1, a link is opened, and event TestEvent is declared. Because the client on server3 has declared interest, a notification message is delivered and reported there.

The client on server4 is next terminated (via close link and control-D). The server4 client is rerun, this time connecting to server2, and the link is opened. The event TestEvent is then declared at server2. Nothing happens at server3, as it is global (not local) to the server on server2.

Finally, the client on server4 declares a global event (GlobalEvent), and the client on server3 is notified. The path is server4 to server2, server2 to server1, and finally server1 to server3.

Both test clients are then terminated via close link and Control-D.

3.1.4.6 Test Client Diagnostics

The test client fev has features whereby it can spy on what notification servers are doing and what the status of each connection is. The commands are

$i : sends back information and statistics
$s : sends back socket connections information
$aux : sends back auxiliary socket connection information
$rem : sends back remote server list
$eve : sends back listing of server's event board

3.1.4.7 Test Client Information Diagnostic $i

Entering $i at the fev test client's terminal causes statistics information to be returned to the client. Example:

```
% fev server1
FEMIS_EVENT port is 9020
$i
FEMIS_EVENT - Version 1.0.11 - Wed Dec 14 15:54:18 PST 1994
started time . . . . . Sat Dec 17 03:00:09 1994
current time . . . . . Mon Dec 19 13:51:59 1994
paid . . . . . 23473
ppid . . . . . 1
uid . . . . . 30508
gid . . . . . 30508
dir . . . . . /home/femis/exe
home . . . . . /home/femis/sunos/home/femisuser
host . . . . . server1
port . . . . . 9020
background . . . . . Yes
accepts . . . . . 192
connects . . . . . 1
reconnects . . . . . 0
messages rcvd . . . . 11826
characters rcvd . . . . 513556
messages sent . . . . 1274
characters sent . . . . 85600
malloc arena/used . . 61448 35416
evtbuf cur/tot/peak . . 2 9 9
evtbrd cur/tot/peak . . 2 9 2
intlist cur/tot/peak . . . 288 2607 306
```

From the display above, you know the following information about the notification server daemon: has been up for 2 days, was started at 3:00 a.m. on Dec 17, is the Dec 14 version; the process ID is 23473; the sever is in background (because ppid == 1); its uid is 30508 (femis account); user's home is /home/femis/sunos/home/femisuser; the host's name is server1; the service port number is 9020 (the standard port); the notification server is running as a clone in background; and the server currently has 35416 bytes of dynamic memory allocated.

Furthermore, the server has accepted 192 connections, has established one connection itself (to the other server), has done no reconnects (because of connection termination), has received 11826 messages containing a total of 513556 characters, and has transmitted 1274 messages containing a total of 85600 characters. Using either received or transmitted, the average message length is approximately 42 characters.

For event library statistics evtbuf, evtbrd, and intlist, also reported are current, total, and peak.

Character and message counts utilized in the diagnostic messages overhead are not included in the totals displayed.

3.1.4.8 Test Client Socket Connections Diagnostic $s

Entering $s at the fev test client's keyboard causes socket connection information to be sent to the test client's display. Example:

```
% fev server1
FEMIS_EVENT port is 9020
$s
```

The heading of the display contains the following:

ii : index number in femis_event's internal database
lisn : 1 if socket is the server's primary listening socket
acpt : 1 if connection was accept()-ed on this socket
conn : 1 if connect() was established on this socket
stio : 1 if this is one of the standard I/o files
svrc : 1 if accept or connect is to another server
chan : the channel number
host : name of the host to which this socket is connected
IP : the IP address to which this socket is connected
hwid : 32 bit hardware id number - derived from IP address
anid : the notification system client id number
when : when (date and time) when connection was established
rcv : number of messages and number of characters received
xmt : number of messages and number of characters transmitted.

Example display of first 11 parameters:

```
ii lisn acpt conn stio svrc chan : host : IP : hwid : anid :
3 1 0 0 0 0 3 : server1.pnl.gov : 130.20.76.45 : 82144C2D : 0 :
4 0 1 0 0 0 4 : server5.pnl.gov : 130.20.28.29 : 82141C1D : 19 :
5 0 1 0 0 1 5 : server2.pnl.gov : 130.20.242.31 : 8214F21F : 0 :
6 0 1 0 0 0 6 : 130.20.28.131 : 130.20.28.131 : 82141C83 : 71 :
7 0 1 0 0 0 7 : server6.pnl.gov : 130.20.60.103 : 82143C67 : 47 :
```

```
8 0 1 0 0 0 8 : server4.pnl.gov : 130.20.92.71 : 82145C47 : 69 :
9 0 1 0 0 0 9 : server3.pnl.gov : 130.20.92.87 : 82145C57 : 0 :
10 0 1 0 0 0 11 : server7.pnl.gov : 130.20.92.39 : 82145C27 : 53 :
```

Example display of final 5 parameters:

```
when : rcv : xmt
Sat Dec 17 03:00:12 1994 : r 0 0 : x 0 0
Mon Dec 19 09:50:29 1994 : r 255 11115 : x 7 473
Sat Dec 17 03:00:24 1994 : r 0 0 : x 4 319
Mon Dec 19 10:47:17 1994 : r 91 3896 : x 8 547
Mon Dec 19 10:27:49 1994 : r 259 11303 : x 8 547
Mon Dec 19 10:45:24 1994 : r 56 2335 : x 2 117
Mon Dec 19 11:14:17 1994 : r 13 13 : x 0 0
Mon Dec 19 10:29:36 1994 : r 56 2335 : x 2 117
```

From the above display, we can say that 5 clients currently have active connections, that client ID numbers range from 19 to 71, and that one client has no entry in the local name table (IP address 130.20.28.131).

Socket 3 is the listening socket. Socket 5 connects to the notification server on server2. Socket 9 is the client doing diagnostics.

Character and message counts utilized in the diagnostic messages are not included in the totals displayed.

3.1.4.9 Test Client Auxiliary Connect Information Diagnostic $aux

Entering $aux at the fev test client keyboard causes the auxiliary connect information to be sent to the test client's display. Example:

```
% fev server1
FEMIS_EVENT port is 9020
$eve
```

The heading of the display that follows contains

```
ii : index number in femis_event's internal database
conn : connect mode = L C A
svrc : server circuit = 0 1
auxtype: aux connection type S C U
host : name of host to which this socket is connected
hwid : 32 bit hardware id number - derived from IP address
port : port number of server/client at remote end
pid : process id number of server/client process at remote end
cid : client id number of server/client process at remote end
```

Example listing:

```
5 L 0 : U : virus.pnl.gov : 8214F20A : 9020 : 14415 : 0
6 C 1 : S : locusts.pnl.gov : 8214F20B : 9020 : 12093 : 0
7 A 0 : U :  : 0 : 0 : 0 : 46
8 C 1 : S : temblor.pnl.gov : 8214F20C : 9020 : 19831 : 0
9 A 0 : U :  : 0 : 0 : 0 : 38
10 A 0 : U :  : 0 : 0 : 0 : 48
11 A 0 : U :  : 0 : 0 : 0 : 43
12 A 0 : C : hattrick : 82145C57 : 9020 : 2593 : 0
```

3.1.4.10 Test Client Remote Servers Diagnostic $rem

Entering $rem at the fev test client keyboard causes the remote connect information to be sent to the test client's display. Example:

```
% fev server1
FEMIS_EVENT port is 9020
$rem
```

The heading of the display that follows contains

```
RemoteServer : Port number @ host name of the remote notification server
IPAddress : IP address of the remote host
Address : 32 bit hardware id number - derived from IP address
```

Example listing:

```
RemoteServer : IPaddress : Address
9022@virus.pnl.gov : 130.20.242.10 : 8214F20A
9021@temblor.pnl.gov : 130.20.242.12 : 8214F20C
```

3.1.4.11 Test Client Event Board Diagnostic $eve

Entering $eve at the fev test client keyboard causes the server's event board information to be sent to the test client's display. Example:

```
fev - test client for femis_event server
FEMIS_EVENT port is 9020
$eve
```

The heading of the display that follows contains

```
EventName : name of the event
ExerID : exercise id
Par1 : first parameter
Par2 : second parameter
```

Par3 : third parameter
GMT : date/time event declared
RecID : record id

Example listing (abbreviated):

MsgName	: ExerID	: Parm1	: Parm2	: Parm3	: GMT	: RecID
CSEPPEvent	: 0	: 10000299	:	: ALL_OVER	: 18:25	: 37
MD2	: 1295	: Operations	:	: UPD:10001	: 18:38	: 41
PLN:PlanChanged	: 0	: 10000107	:	:	: 18:17	: 33
PLN:TaskChanged	: 0	: 10000006	:	: 21	: 16:17	: 23
RSB:EventLogAdd	: 0	: J	: AckEvent	:	: 18:25	: 39
RSB:EventLogAdd	: 1295	: J	: D2:10001	:	: 18:37	: 40
Udept	: 0	:	:	:	: 15:19	: 19
Ufacility	: 0	:	:	:	: 15:16	: 18
UlocalID	: 0	: TEADTEAD	: alstuff	:	: 15:48	: 43
Uperson	: 0	:	:	:	: 16:48	: 24

3.1.4.12 Test Client Synchronize Action $sync

Entering $sync and a qualifier at the fev test client keyboard causes the server to send the same message back to fev, which can utilize reception of known dollar-sync messages to synchronize certain events and actions.

The test client uses the command **$sync exit** to synchronize forced exit while running in script mode, which must be used in conjunction with the -x option.

Example script:

```
#!/bin/csh -f
#
fev -x virus 9020<<eod
o
g My-Event 1 "par one" par_two par3
g My-Event 123 "" - 999.000
g Your-Event 99 - - -
c
\$sync exit
eod
```

The above script runs fev, opens a link, declares the three events, closes the link, and synchronizes a forced exit.

3.1.4.13 Data Driven Notification Command Line Arguments

A Data Driven Notification (DDN) command line interface has been added to fev. This feature now allows a single event including DDN parameters to be constructed and sent by fev, based solely on new command line arguments. The presence of DDN command line arguments signals fev to utilize single event mode, instead of entering interactive mode.

Following are DDN command line arguments for fev:

Argument	Function
-global	This is a global event
-nopost	Do not post this event
-aux	Call an auxiliary process
-host HOST	Name of host to receive this event
-port PORT#	Port # or protocol # to receive this event
-msgname MSG	Message name
-msgflags FLAGS	Message flags
-origin ORIGIN	Origin field
-exerid EXERID	Exercise ID
-auxprocessidnet AUXID	Auxiliary process id (in femis_event.conf)
-parm## PARM##	Parameter no. ## (up to 50)

3.2 PC Notification Service

3.2.1 PC Notification Service Overview

This section describes the PC Notification Service, which serves as the PC workstation component of the FEMIS Notification Service. The PC Notification Service is designed to provide a path for sharing notification information between PC applications, PC workstations, and UNIX notification servers. Events posted by applications within a PC workstation are first sent to all notification clients on that PC, then forwarded to a UNIX notification server for distribution to other workstations and other notification servers.

The PC Notification Service operates in the background and provides services to PC applications through function calls and window messages. There is no direct user interface except the Notification Service log window, which displays diagnostic messages as the service is running.

The PC Notification Service is implemented as a stand-alone service and is automatically activated when client applications are started and remains active until all clients have been closed. There are no separate startup or shutdown procedures. Instead, notification startup and operations are controlled through configuration files and client function calls, not through command-line options.

3.2.1.1 Executable Binary Files

The PC Notification Service has two executable binary files:

FNOTIFSV.EXE	Notification Service executable
FNOTIF32.DLL	Notification Service function library

These files are normally located in the WINNT\SYSTEM32 directory but may be placed elsewhere, as long as they can be found on the system search path.

3.2.1.2 Notification Service Startup

Since the Notification Service is started by the Notification Service DLL, the user has no control over startup operations. Instead, startup parameters are read from a configuration file and can be adjusted to suit the needs of a particular installation.

3.2.2 PC Notification Service Configuration Options

The PC Notification Service can be customized by modifying one or more configuration parameters. These parameters allow you to change Notification Service behavior to accommodate client needs and special requirements. For instance, a remote user connected via a modem may need to increase the timeout limit for notification server connections, or a stand-alone installation might want to disable all network monitoring. Each of these requirements can be satisfied by adjusting the configuration parameters to fit the client's needs.

3.2.2.1 Configuration Parameters

Each configuration parameter has a unique name and most have a default value. The available configuration parameters are as follows:

Parameter	Purpose	Default Value
RunAsStandAlone	StandAlone flag (True/False)	False
SocketMaxWait	Socket timeout value (seconds)	10
LostConnCheckInterval	Lost connection check (seconds)	30
LostConnRetryInterval	Lost connection retry (seconds)	30
EventQueueSweepInterval	Queue sweep interval (seconds)	1
DefaultNotifServerHost	Default server host name	none
DefaultNotifServerPort	Default server port	none

If the default value for a parameter is not satisfactory, you can assign a more suitable value. However, you must be careful that the new value is reasonable and does not have an adverse effect on Notification Service operation.

3.2.2.2 Notification Service Configuration File

Notification Service configuration parameters are specified in a configuration file, FEMIS.INI, usually located in the Windows NT home directory. Each configuration parameter is specified by a key and its associated value, grouped under the [Notification Service] section.

A typical INI file might look like this:

```
[Notification Service]
;---Notification configuration parameters---
;RunAsStandAlone = False
LostConnCheckInterval = 10
LostConnRetryInterval = 60
```

To create an entry for a configuration parameter, insert a new line that specifies the parameter's name and its new value, separated by an equals sign (=). Key names are not case sensitive, and all blank padding is ignored.

To disable an entry, put a semicolon as the first non-blank character in the entry, which causes the line to be treated as a comment and ignored in all parameter processing.

3.2.2.3 Command-line Options

The PC Notification Service has no command-line options.

3.2.2.4 Environment Variables

No environment variables are used by the PC Notification Service.

3.2.2.5 Host Server Name and Port

UNIX host server name and port number are set by client function calls and are not directly controlled by configuration options. However, clients can use the DefaultNotifServerHost and DefaultNotifServerPort configuration parameters to store server identification information.

Note: FEMIS does not support concurrent connections to multiple notification servers. Only one server can be connected at a time.

3.2.3 PC Notification Service Operation

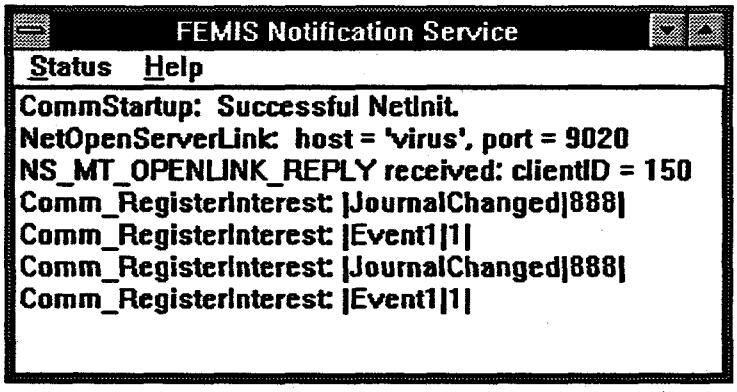
Operation of the PC Notification Service is discussed in the following sections.

3.2.3.1 Notification Service Window

The Notification Service window enables a user or administrator to view information about notification system operations. This window provides information about the system status and current version, along with a log of recent diagnostic messages. When this window is minimized, its icon indicates the current Notification Service status:

Stand-alone	-	blue icon with red border
Connected to server	-	blue icon with black border
Lost connection	-	blue icon with red slash across it

Figure 3.1. FEMIS Notification Service Window



For status information, select Notification Status under Status on the menu bar. This activates the Notification Status window, which displays information about local and server status, client count, event count, server host name, and server port number. The Notification Status window updates itself automatically, so its information remains current even if the window is left open.

For version information, select About Me under Help on the FEMIS menu bar. This activates the About Me window, which contains version and copyright information.

For diagnostic information, consult the main Notification Service window. This window displays recent diagnostic and error messages, including network messages to and from the server and attempts to restore lost server connections.

3.2.3.2 Lost Connections

Lost connections with the UNIX notification server are a common problem and occur for a variety of reasons. The PC Notification Service is designed to automatically detect and restore lost connections, with minimal impact on FEMIS software operations.

Whenever a lost server connection is detected, the PC Notification Service sends a diagnostic message to the log window, activates the Lost Connection icon, and goes into restoration mode. Every few seconds, as specified by the LostConnRetryInterval value, the Notification Service attempts to contact the server and restore the connection. During this time, local notification still occurs, but all messages to and from the server are lost and cannot be recovered. When the server finally answers, the connection is restored and the Notification Service returns to normal operation.

As discussed in Section 3.2.3.1, Notification Service Window, you can use the status icon or status window to monitor lost connections.

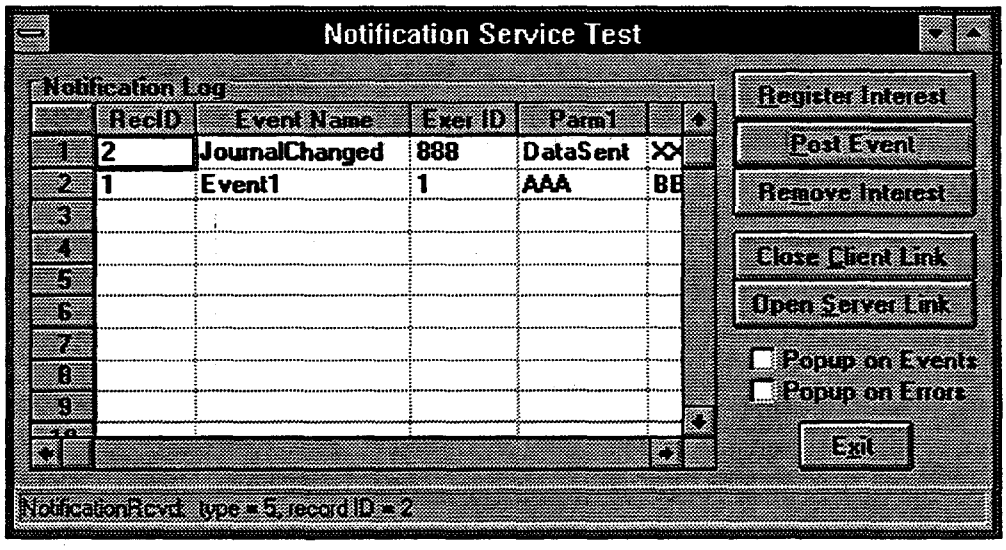
3.2.4 PC Notification Test Client

3.2.4.1 PC Test Client – NOTITEST.EXE

The PC Notification Test Client, NOTITEST.EXE, is included in the FEMIS installation and can be used to test notification functions and diagnose notification problems. This program enables a user to manually post notification events, monitor events generated by other applications, and force notification errors for testing purposes. See the Section 3.2.4.4, PC Test Client Functions, for more information.

At startup, NOTITEST automatically establishes a notification client link and registers an interest in the Event() 1 : 1 event. It also enables notification loopback so it can receive its own events. However, NOTITEST starts in stand-alone mode, without connecting to a UNIX notification server. Use the Open Server Link function if you wish to open a link to your notification server.

Figure 3.2. Notification Service Test Window



3.2.4.2 PC Test Client Configuration

The PC Test Client has no configuration options or other means to customize its default behavior. However, the test functions (below) can be used to change client behavior at runtime.

3.2.4.3 PC Test Client Command-line Options

The PC Test Client has no command-line options.

3.2.4.4 PC Test Client Functions

The PC Test Client offers a variety of functions for testing the Notification Service. These functions are accessible through command buttons on the test client user interface window.

Open Client Link
The Open Client Link function opens a notification client link, allowing the test client to register interests and post notification events. This function is enabled only if there is not an existing client link.

Close Client Link
The Close Client Link function closes the existing client link to the Notification Service, disabling client notification, and discarding all interests registered by the client. This function is enabled only when there is an existing client link.

Open Server Link
The Open Server Link function opens a link between the PC Notification Service and a named notification server. The user is prompted for the server name and port number. When the user clicks the OK button, the Notification Service closes the previous server link (if any) and sends a connection request to the new notification server.

If the server is available, a connection is established and this server becomes the notification server for this PC. If the server is not available, the Notification Service will ask whether you wish to retry the connection. If you select Yes, the Notification Service will treat the problem as a lost connection and go into restoration mode. Otherwise, the Notification Service will go into stand-alone mode and operate without a server connection.

This function is enabled at all times and is useful for testing server connections and simulating lost connections.

Register Interest
The Register Interest function enables the test client to register an interest in one or more notification events. The user is prompted for an event name and exercise number that uniquely identify a notification event. When the user clicks the OK button, the test client registers an interest in the specified event and begins to log all notifications for that event.

This function is very useful for troubleshooting notification problems because it allows the user to monitor notification events posted by other applications. For instance, if an application is not responding to a specific sequence of notification events, the test client program can register an interest in those events and verify that the events are being sent in the correct order.

This function is enabled only when the test client has a valid client link.

Remove Interest
The Remove Interest function enables the test client to remove an interest in one or more notification events. The user is prompted for an event name and exercise number that uniquely identify a notification event. When the user clicks the OK button, the test client removes its interest in the specified event and is no longer notified about that event.

This function is enabled only when the test client has a valid client link.

Post Event
The Post Event enables the test client to post a notification event and simulate events posted by other applications. The user is prompted for the event name, exercise number, and three event parameters, along with control flags that determine how the event will be processed. When the user clicks the OK button, the test client sends this event to the Notification Service for distribution to other local and remote clients.

This function is very useful for troubleshooting notification problems because it allows a user to simulate notification events posted by other applications. For instance, the test client can post a specific sequence of notification events and verify that other applications respond correctly to that sequence.

This function is enabled at all times.

Popup On Event
The Popup On Event option is used to alert the user each time the test client receives an event notification. This allows the test client to function as an event monitor by displaying a popup message box whenever an event is received. This function can also test the Notification Service queuing functions by introducing a user-controlled delay into the event processing system.

Popup On Errors
The Popup On Errors option facilitates error-handling tests by displaying a popup message each time an invalid notification message is received.

3.2.4.5 PC Test Client Diagnostics

The PC Test Client does not include any diagnostic functions.

3.2.5 Notification Server Troubleshooting

The notification server is very stable; however, this program runs in a network environment and, thus, is prone to any and all failures that can occur in network computing and distributed data management systems.

3.2.5.1 Check Notification Server Active

To check if the notification server is active, log in to the UNIX server and issue the following command:

```
%/usr | ucb | ps axw | grep femis_event
```

If the notification server is active, you will get a reply such as:

```
17739 pe S 0:00 femis_event -c server1 -e femis_event.e.log.941219.1140

1073 pe S 0:00 grep femis_event
```

If the notification server is not active, only the second line above will be displayed. The process identification (PID) number of the femis_event notification server is the first number shown, e.g., 17739.

3.2.5.2 Check Notification Server Communication

To check the notification server communication, run the UNIX test client either from the server host or from another UNIX system. You should be able to run fev and issue notification server instructions. Example:

```
% fev
```

If the notification server is not active, you will get a reply such as the following and then be returned to the command-line processor:

```
fev - test client for femis_event server
FEMIS_EVENT port is 9020
connect failed: Connection refused
%
```

If the notification server is active, you should get a reply such as the following:

```
fev - test client for femis_event server
FEMIS_EVENT port is 9020
```

After receiving the above reply, you can issue an instruction to the UNIX test client. Example:

```
o
```

This is the test client's command to open a link. Next you should see

```
<<<<<< received OPENLINK-reply: client-id = nnnn
```

where nnnn is an open link ID number (could be any positive integer).

If you get such a reply, the notification server is active and communicating. If the notification server is active and communicating, then the problem is probably either in the network or on the PC side.

3.2.5.3 Aborting Notification Server

If you need to abort the notification server during testing or troubleshooting, you must manually log in as the user account from which femis_event was started. In FEMIS, the user account is femis, or you can log in as superuser.

You next need to learn the PID number of the femis_event server needing to be killed. There are two ways to learn the PID of a FEMIS server process.

The first is to use the ps and grep commands. Example:

```
%/usr | ucb | ps axw | grep femis_event
```

If the notification server is active, you will get a reply such as:

```
23473 pe S 0:00 femis_event -c server2 -e femis_event.e.log.941219.1140
1073 pe S 0:00 grep femis_event
```

If the notification server is not active, only the second line above will be displayed. The PID of the femis_event notification server is the first number shown, e.g., 23473.

The second way to learn the PID of femis_event is to run the test client and use the $i spy command. Example:

```
% fev - # connect to local host
fev - test client for femis_event server
FEMIS_EVENT port is 9020
$i
pid . . . . . 23473
```

From the $i reply, the femis_event pid is 23473.

With the PID number, you can abort the notification server. The preferred way is

```
% kill -2 23473
```

Recheck if the server is still active. If the above kill -2 (the graceful exit), did not work, then use

```
% kill -9 23473
```

Using kill -9 will kill the notification server, but the state of open connections will be lost and possibly may not be recoverable until some long TCP/IP timeout period elapses.

A script file, such as the following, may be used

```
foreach killnum ( -2 -9 )

ps ef >! ..PS..

set serverpid = ( `fgrep femis_event ..PS.. | awk `{print $2}' ` )
foreach pid ( $serverpid )
echo kill $killnum $pid
kill $killnum $pid
end

end
```

3.2.5.4 Fixing Notification Port

When running a FEMIS client application such as a Visual Basic application, the application first uses the FEMIS.INI file in the Windows directory to get the notification server's name and port number. If either the name or port number is incorrect, you will get an error 10054. You could fix the file to avoid this error occurring in the future; but it is not necessary because the Visual Basic application then lets you login to an EOC and gets a new notification server name and port number from the FEMIS database. If either the new name or port number is incorrect, you will get an error 10054. You must then correct the EOC table by changing the values for either the EOC_SERVER_NAME or the EOC_NOTIFY_PORT fields.

3.2.5.5 PC WinSock Errors

The following list includes the errors encountered during development and testing of the notification server software. A complete list of WinSock and UNIX errors can be found in *Windows Sockets, Version 1.1* documentation.

PC WinSock Error 10022
This error is an internal Windows Sockets error which is caused when a Windows application crashes/terminates without properly closing down. In doing so, the Windows application has wasted and lost critical dynamic memory. Error 10022, which means invalid argument, is reported by mistake. The real problem is Windows running out of a critical resource. Shut down other Windows applications and reboot the PC.

PC WinSock Error 10024
This error is an internal Windows Sockets error which is caused when a Windows application crashes/terminates without properly closing down. In doing so, the Windows application has wasted and lost critical dynamic memory. Error 10024, which means too many files open, is reported by mistake. The real problem is Windows running out of a critical resource. Shut down other Windows applications and reboot the PC.

PC WinSock Error 10038
This error is an internal Windows Sockets error which is caused by a software error, most likely manifested from Windows running out of a critical resource. In reaching this error, an application has tried to reuse an I/O channel which was previously connected to a network socket but has since been closed. Restart the affected applications. If this does not fix the problem, reboot the PC.

PC WinSock Error 10050
This error means the network is down; there is no network communication with the server host to which this PC is trying to connect. Report the error to the System Administrator and wait for a diagnosis. After all hardware and communication bugs have been fixed, restart the affected applications. If this does not fix the problem, reboot the PC.

PC WinSock Error 10053
This error means that connection to the server was aborted and may be because the server was terminated, either intentionally or by a failure. This error can also mean that connection was never established because the server is not currently active. Check if the notification server, femis_event is currently active on the UNIX server. If not, restart it using scripts described in Section 3.1.1.3, Daemon Server Startup. The UNIX test client can be used to check for server health, see Section 3.1.4, Notification Server Utilities.

PC WinSock Error 10054
This error means that the notification server is not active. Check if the notification server, femis_event is currently active on the UNIX server. If not, restart it using scripts described in Section 3.1.1.3, Daemon Server Startup. The notification subsystem UNIX test client can be used to check on server health, see Section 3.1.4, Notification Server Utilities.

This error can also mean that the client software on the PC does not have the correct service port number or server. The default port for the notification server is 9020. Client software must use this same service port. If the port number is determined to be incorrect, fix it and restart the client software applications. Reboot the PC if necessary.

3.3 Starting/Stopping Notification Service

When the server is rebooted or shutdown, it runs the /etc/init.d/femis script, which start or stops the Notification Service using the following scripts in the /home/femis/bin directory.

3.3.1 Starting Notification Service

The /home/femis/bin/start notify script uses the EOC List File (./etc/eoclist.dat) to determine how to start the Notification Service. The file tells how many Notification Service processes to start, which ports to use, and which other Notification Services to communicate with. You can run the following script.

```
% startnotify
```

If the Notification Service(s) is already running, you cannot start new ones.

To start Notification Service(s) with logging turned on, you can run the following script:

```
% startnotify -log
```

3.3.2 Stopping Notification Service

The /home/femis/bin/stopnotify script stops the Notification Service(s) by finding all processes running the femis_event program and then kills them using kill -2. You can run the following script.

```
% stopnotify
```

4.0 FEMIS Command Server

Command server online documentation is provided in three man pages on the UNIX server. Log onto the EOC's server as femis and enter:

```
% man cmdservd
% man cmdserv.conf
% man cmdserv
```

cmdservd is the command server daemon. cmdserv.conf is the command server configuration file. cmdserv is a UNIX test client for the command server.

4.1 cmdservd – FEMIS Command Server Daemon

4.1.1 Synopsis

```
cmdservd [-conf config-file]
cmdservd [-conf config-file] [-v] [-syntax [-show] [-check]]
```

4.1.2 Availability

The FEMIS command server daemon cmdservd executable, configuration file, test client, and related files are included with the FEMIS application. The default locations for these files are /home/femis/bin and /home/femis/etc on the FEMIS UNIX data server.

4.1.3 Description

FEMIS utilizes remote command servers, executing on a UNIX host computer so PC workstation users can launch large mathematical model/simulation programs. These include the Evacuation SIMulation (ESIM), a module in the Oak Ridge Evacuation Modeling System (OREMS).

The command server is also utilized in certain FEMIS system administration functions, e.g., starting-stopping notification.

A high degree of security is realized in this command server because:

- Security problematic command servers such as rsh and .rhosts are not used. A client node need not be a trusted host.
- A command server runs only as a non-privileged, non-root process.
- A command server is forked as a child of *inetd*, eliminating the need to maintain socket connections.

- The command server does not execute raw UNIX commands. Rather it looks up necessary commands in a configuration file and matches parameters with arguments based on messages from the client.

- The command server is very limited in what it can do. Only those commands and functions defined in the cmdserv.conf configuration file can be invoked.

- Files written are only those temporary and output files written by the target executable. All communication between command server and forked process takes place via memory and unnamed pipes only.

- Passwords and other sensitive data are sent on the client-to-server socket encrypted. Clear passwords are never sent to the application on the command line to possibly be displayed by ps.

- The user and client machine making requests to run programs on a command server are verified prior to running any entry. Several methods are utilized to block requests from anyone except authorized users.

4.1.4 Options

The command server has two basic execution modes: daemon and command line. In daemon mode, execution is started and controlled by the *inetd* Internet daemon and runs as a detached process. In command line or interactive mode, cmdservd runs in response to a user entry. Command line mode is used mainly to check on the syntax of new configuration files.

The default configuration file name is cmdserv.conf, and its default path is /home/femis/etc. To change either the configuration file name or path, use the -conf option. Possible formats for use with the -conf option are as follows:

```
1% cmdservd -conf filename
2% cmdservd -conf subdirectory/
3% cmdservd -conf subdirectory/filename
4% cmdservd -conf /fullpathname/
5% cmdservd -conf /fullpathname/filename
```

Case 1 Syntax contains no slashes (/), and thus no path or directory names. The argument to -conf is the name of a file which resides in the default configuration directory /home/femis/etc.

Case 2 Syntax is in subdirectory format and contains a slash (/) as the last character. The first character is not a slash and comma (/,) thus a relative path and not an absolute path. The described syntax tells cmdservd to use the default file name in a subdirectory of the default path.

Case 3 Syntax specifies a subdirectory and file name. The named file is thus located in the subdirectory of the default path.

Case 4 Syntax specifies to look for the default file name cmdserv.conf in the full path specified in the option. Both first and last character of the option are slashes (/).

Case 5 Syntax specifies a full path and file name. None of the defaults apply in this case.

Option -v asks cmdservd to display its version information. Example:

```
virus% cmdservd -v
cmdservd version 1.0 - Wed Feb 14 14:41:00 PST 1996
```

Option -syntax invokes only the cmdservd syntax checker.

Options -show and -check are used in conjunction with -syntax.

The -syntax -check options cause cmdservd to process the configuration file, checking for syntax problems. Options -syntax -show cause cmdservd to compile the configuration file, check for syntax problems, and display the resulting linked structure.

4.1.5 Syntax Check

To check the syntax of a command server configuration file, enter the options -syntax -check to cmdservd, examples:

```
1% cmdservd -syntax -check        # check default
2% cmdservd -syntax -check -conf CFG # check CFG file
```

The following format is output by -syntax -check. Any line detected with suspect syntax is reported.

```
Line ##: line-from-file
    error-message
    error-message
```

where ## is the line number, line-from-file is the text from the configuration file at line ##, and error-message is a list of error messages describing the problems. Example:

```
Line 13: badnews
    invalid block/directive type code
```

The following list provides all possible error messages and their probable cause.

invalid block/directive type code

A block name or directive name is not one of those allowed. The block names are ALL, ACCESS, HOST, SITE, and ENTRY. Directive names are site, deny, allow, executable, directory, password, outfile, errfile, argument, environment, file, and put.

block requires no parameters

The ALL and ACCESS blocks do not require a list of parameters, i.e., [BLOCKNAME par1 par2 ...].

block requires exactly 1 parameter

The ENTRY block requires exactly one parameter which is the entry item name, e.g., [ENTRY abc], where abc is the name of a program.

block requires 1 or more parameters

The HOST and SITE blocks require at least one parameter which is a list of host or site names. HOST and SITE cause conditional compile. If the current host or site is the same as an item in the list, compilation continues. Otherwise, compilation of this program block is blocked.

directive not valid outside a block

All directives must be contained inside a block.

ENTRY block can not include other blocks

It is invalid for an [ENTRY ..] block to contain other blocks (at this time).

directive must be inside HOST block

The site directive is only valid inside a HOST block.

directive must be inside ACCESS or ENTRY block

The allow and deny directives are only valid inside for an ACCESS or ENTRY block.

directive must be inside ENTRY block

Directives executable, directory, password, outfile, errfile, file, put, and argument are only valid inside an ENTRY block.

environment must be inside ENTRY ALL SITE or HOST block

The environment directive must be inside of an ENTRY, ALL, SITE, or HOST block. When inside ENTRY, the variable is evaluated for that entry item only. When inside ALL, SITE, or HOST, the variable is evaluated whenever the block condition is TRUE, and not evaluated if the block condition is FALSE.

ACCESS block can only contain deny and allow

An ACCESS block can not contain anything but deny and allow.

site requires exactly 1 parameter

Site directive requires exactly one parameter. Zero parameters and two or more parameters are invalid syntax.

directive requires 1 or 2 parameters

Allow and deny directives require exactly one or two parameters. Zero parameters and three or more parameters are invalid syntax.

invalid character(s) in IP address field

Internet Protocol (IP) address field in the deny and allow directives can contain only digits 0-9 and the period (.) characters. Anything else is invalid syntax. A format specification is not valid in allow or deny directives.

invalid character(s) in IP subnet mask

IP subnet mask in a deny or allow directive can contain only digits 0-9 and the period (.) characters. Anything else is invalid syntax.

invalid IP address

IP address numbers must be in the range 0-255.

invalid IP subnet mask

Only the numbers 255, 254, 252, 248, 240, 224, 192, 120, and 0 are valid IP subnet mask elements. The value 0 must be followed by 0. The value 255 must be preceded by 255. A value not 0 or 255 can appear only once. For example, 255.255.255.192, 255.255.255.0, 255.255.128.0.

directive requires format [parameters]

Directives executable, directory, password, outfile, errfile, file, put, argument, and environment require a format string and an optional list of parameters. Examples:

```
executable /home/femis/bin/command/xyz
directory  /home/femis/user/%s/ DIRECTORY
```

only %s allowed in format

Format strings in this language allow only the %s printf conversion. Conversions, such as %d, %x, and %u are not allowed.

format and number of parameters do not match

The number of parameters included and the number required by the format string do not agree.

executable path/file affected by client

Structure of the configuration file program that generates the executable path/file string is affected by external environment variables sent in the client message. Such affects are illegal. Executable must be developed only from static values and environment variables local to the configuration file.

password affected by client

Structure of the configuration file program that generates the password string is affected by external environment variables sent in the client message. Such affects are illegal. The password must be developed only from static values and environment variables local to the configuration file.

4.1.6 Installation

The installation process copies files cmdservd, cmdserv, and cmdserv.conf to directory /home/femis/bin and home/femis/etc. There files are required to be at this path, unless modifications are made to the /etc/inetd.conf and cmdserv.conf files.

FEMIS installation adds the following line to the /etc/services file to define the command server service port name.

```
femis-cmdserv  9015/tcp  fxcmdserv  # command server
```

FEMIS installation adds the following single line to the /etc/inetd.conf file to add the command server to the *inetd* Internet daemon.

```
fxcmdserv stream tcp \
    nowait femis /home/femis/bin/cmdservd cmdservd
```

4.1.7 Protocol

Only Transmission Control Protocol (TCP) connection and reliable messages are ever used in the FEMIS command server daemon (femiscomd). User Datagram Protocol (UDP) is not used.

The FEMIS command server and a client program carry on a two way half duplex conversation. After successful connection has completed, the server and client exchange hello messages. The server hello message contains encryption seeds for the session. The client hello message contains optional mode flags, used to characterize certain server-client exchanges.

Once hello messages have been exchanged, cmdservd then listens for command messages from the client which contain the necessary parameters and instructions for running a specific program on the UNIX server.

After receiving a command, the command server looks for that entry in the configuration file. Actual UNIX commands and the format of arguments come from the configuration file, not from the socket input.

After completing the set up for a computation, the femiscomd forks and executes the specified executable and then goes back to listening for client commands.

4.1.8 Messages

This section describes messages that pass between server and client over TCP socket connections.

4.1.8.1 Message Format

Messages to/from command server and its client have the following general format.

<op:OPERATION|...|...|...><NEWLINE>

Every message begins with < and ends with > followed by an end-of-line. Only characters between < and > have any meaning. The end-of-line character, and anything between > and < have no meaning and should be ignored by both client and server.

Between < and > are an unspecified number of fields, the first one being the operation field. Fields are separated by the pipe (|) character. Fields can contain any number of characters or may be empty, i.e., ||.

Within a field, four characters are escaped: < > | and \. The back slash (\ ) is the escape character.

Note: The field separators < > and | never appear in a correctly encoded field.

The following mappings apply.

Decoded	Encoded
<	\L
>	\R
|	\D
\	\E

4.1.8.2 Message Fields

All message field identifiers are two lower case characters followed by a colon. The identifiers are as follows:

Field	Contents
op:	Operation or function name
ac:	Action code: run, status, kill
pw:	Password field
ev:	Parameter (environment) values
rc:	Return code
er:	Error code
k0:	Key #0 for light encryption (not used)
k1:	Key #1 for light encryption (not used)
k2:	Key #2 for light encryption (not used)
mo:	Modes: alert test ... (client hello only)

4.1.8.3 Operation Codes

The current message operation codes currently are implemented in the command server, the command server's test client, or both:

Code	Description
op:SVRHELLO	Server hello
op:CLIHELLO	Client hello
op:MISCINFO	Miscellaneous info
op:EOF	End-of-file
op:COMMAND	Command directive
op:HELP	Help
op:HELPINFO	Help information
op:QUIT	Quit
op:ERROR	Error to client
op:REPLY	Reply to client
op:ALERT	Alert the client

4.1.8.4 Command Message

<op:COMMAND|ac:ACTION|pw:PASSWD|ev:PAR1|ev:PAR2|...>

where ACTION is run ENTRY, status, or kill; PASSWD is a password string; PAR1 and PAR2 are parameter defines; and ENTRY is the name of an entry in the configuration file.

This message is constructed by the client and sent to the server. It tells the server what entry from the configuration file to invoke. It tells the server what values to use for arguments and environments.

The PASSWD password string should be blank if the entry contains no password definition. If password is present, it must be a 16+ characters password value. The first eight characters are the HWID hex value.

The next eight characters are the client port hex value. Following characters are the user's password string.

Parameters are utilized in the command server as environment variables. Each parameter specification PAR1 PAR2 defines an environment variable, e.g., X=1, CRANK=24-99, NAME=xyz, DB=CTOO. The environment variables thus defined are passed to the configuration file processing and become inputs for building application arguments, input files, and environment. Also see *cmdserv.conf* man page.

4.1.8.5 Error Messages

<op:ERROR|er:MESSAGE>

where MESSAGE is the error message from the command processor.

The following lists possible errors.

can't access client data
can't access client data: PERROR
- Call to getpeername(socket) failed.
- PERROR is message returned from perror().

config file open failed
config file open failed: PERROR
- Open the configuration file failed.
- PERROR is message returned from perror().

config file syntax error on lines LINELIST
- Execution of command server has been terminated because there is one or more syntax errors in the configuration file.
- LINELIST is a list of line numbers with errors.
- Correct the syntax errors and retry. Use -syntax and -check options to see details of the syntax problems.

access denied
- The configuration file allow and deny directives in ENTRY or ACCESS block on the server host ban this command (or all) from client's IP address.

invalid command
- Content of message is not a valid command.

no action
- No valid action was specified.

no password
- A password is required and none was sent.

wrong password prefix
- Either HWID or PORT has wrong value.

unknown action
- Action code in COMMAND message not valid.
- Valid actions are run status kill.

wrong password
- Password supplied is not one required by configuration file.

can't set directory
can't set directory: PERROR
- Cannot change directory to the one specified.
- PERROR is message returned by perror().

already active
- The command server daemon is already executing a process. Either kill or wait for alert.

can't execute program
- Either fork() or execvp() failed. This probably happened because there's something wrong with the executable file or the name specified.

no executable
- The named executable file was not found. There may be something wrong with the path, or the file name.

4.1.8.6 Reply Messages

<op:REPLY|rc:MESSAGE>

where MESSAGE is the reply message from the command processor.

The following lists possible replies.

successful
- command completed successfully

finish TIMESTAMP IDENT
- STATUS is execution finished
- TIMESTAMP also used in log file names
- IDENT is the UNIX process id number

killed TIMESTAMP IDENT
- STATUS is execution killed
- TIMESTAMP also used in log file names
- IDENT is the UNIX process id number

active TIMESTAMP IDENT
- STATUS is execution still in progress
- TIMESTAMP also used in log file names
- IDENT is the UNIX process id number

not active
- No process has been executed.

Alert Message

<op:ALERT|rc:MESSAGE>

where MESSAGE is the process completion status:

finish TIMESTAMP IDENT
- STATUS is execution finished
- TIMESTAMP also used in log file names
- IDENT is the UNIX process id number

killed TIMESTAMP IDENT
- STATUS is execution killed
- TIMESTAMP also used in log file names
- IDENT is the UNIX process id number

4.1.8.7 Message Example

```
From server     From client
<op:MISCINFO|ITEM1|ITEM2|...>
<op:SVRHELLO|k0:|k1:|k2:>
                <op:CLIHELLO|k1:|k2:|mo:alert>
                <op:COMMAND|ac:run test|
                        pw:|ev:A=73|ev:B=Dog|ev:X=Cat>
    <op:REPLY|rc:active 9602141130 12933>
                <op:COMMAND|ac:status|pw:>
    <op:REPLY|rc:active 9602141130 12933>
                <op:COMMAND|ac:status|pw:>
    <op:REPLY|rc:active 9602141130 12933>
    <op:ALERT|rc:finish 9602141130 12933>
```

4.1.9 Service Port and Name

The cmdservd service port number currently is 9015. The short name is femis-cmdserv or fxcmdserv.

4.1.10 Files

Files utilized during the installation and execution of the FEMIS command server include the following:

- /home/femis/bin/cmdservd daemon executable
- /home/femis/etc/cmdserv.conf configuration file
- /home/femis/bin/cmdserv test client (UNIX)
- /etc/services service port numbers
- /etc/inetd.conf internet daemon config

4.2 cmdserv.conf – FEMIS Command Server Configuration File

4.2.1 Availability

The FEMIS command server configuration file cmdserv.conf is included with the FEMIS application. The default location of the file is /home/femis/etc on the FEMIS UNIX data server.

4.2.2 Description

This configuration file provides specific configuration information to the FEMIS command server daemon cmdservd. Unlike problematic remote compute servers such as RSH, the FEMIS command server provides some degree of security through this configuration file.

Security is also realized by placing severe limits on what this command server is allowed to do. Only those procedures defined in the configuration file can be spawned.

Additional security is realized through an encrypted password mechanism. Cmdservd currently uses simple encryption, with RSA or SSL planned for the future.

The FEMIS project, and a CSEPP site administrator have the ability to configure allowed and denied clients on a per site basis. Allow and deny directives give the administrator the ability to allow individual workstations in the local Emergency Operation Center (EOC), or a remote EOC, but deny all others. Specification of allowed and denied workstations is based on IP address.

The processes used in the command server daemon to parse its configuration file are similar to how LEX/YACC generated parsers work. In LEX, a parser reads text according user defined rules. Output of the LEX analyzer is handed to the compiler YACC that builds a complex linked structure. The linked structure provides a simple mechanism for the process to scan the input program, without having to reread and reparse the input files.

In the command server daemon, the source code is read by a text parser function. This parser recognizes only two general source constructs: block and directive. Block is the outer level construct, and directive the inner level. A block can contain other blocks or directives. Directives are stand-alone—do not contain other directives or blocks.

4.2.3 Syntax

A configuration file contains block, directive, and comment syntax constructs.

A line starting with a # character in column 1 is a comment. Any # character, not part of a string, begins a comment to the end of that line. Example:

```
# a comment line
argument %s XYZ  # comment to end-line
argument %s YZX  # another comment ...
```

A block identification begins with the [(left bracket) character and ends with] (right bracket). All blocks are terminated by [END]. General block syntax is as follows:

```
[BLOCK]  or  [BLOCK parameters]
...          ...
[END]        [END]
```

Directive lines begin with a keyword, followed by zero or more parameters. Directive parameters can be additional keywords, or a quoted string. General directive syntax is as follows:

```
directive
directive parameter
directive format-string
directive format-string parameters
```

General syntax of a command server configuration file is as follows:

```
# comments
[BLOCK declaration]
directives
more blocks
[END]
more blocks
```

4.2.4 Block Syntax

The command server configuration language utilizes five block types: ACCESS, ENTRY, HOST, SITE, and ALL. A block statement always begins with the [(left bracket) character, followed by the block type name. Whether parameters are required is a function of block type.

The block types and their summary purpose are as follows:

Block Type	Purpose
[ACCESS]	Begin access specification block
[ENTRY entname]	Begin entry block (conditional)
[HOST hostlist]	Begin host block (conditional on host)
[SITE sitelist]	Begin site block (conditional on site)
[ALL]	Begin unconditional block
[END ...]	Marks end of a block

In ACCESS block, a parameter after the block type is not required nor is one allowed. Likewise, the ALL block does not require a following parameter, nor is one allowed.

An ENTRY block requires one and only one parameter, the entry name.

The HOST and SITE blocks require a list of one or more parameters, where the parameters are names of hosts or names of sites.

The END statement must have the characters [ENDxxx], where xxx is zero or more unprocessed characters, i.e., the parser scans only for [END. Characters xxx are only for commentary purposes, i.e., [END of block]. Every block must be terminated by an [END] statement, which marks the end of the block.

A simple example of command server configuration file structure follows:

```
#
# a comment line
#
[HOST princess queen]    # if host is princess or queen
[ENTRY travelcost]       # then define entry travelcost
...
[END of travelcost]
[ENTRY distance]         # and define entry distance
...
[END of distance]
[END of princess queen]
```

A detailed description of each block type follows:

4.2.4.1 ACCESS Block

Through an ACCESS block, the FEMIS project or a CSEPP site administrator can configure allowed and denied access to command server resources on a site's UNIX data server.

Two (and only two) directives are permitted in an ACCESS block: allow and deny. The ENTRY block also permits allow and deny directives.

When allow and deny appear in an ENTRY block, they specify what workstations can execute the specific entry. When allow and deny appear in an ACCESS block, they specify what workstations can execute any entry in the configuration file. An ACCESS block may be placed inside of HOST or SITE blocks, thus adding site-by-site conditional use.

The parameter of allow and deny directives are in the form of an IP address. This parameter can be in the form of a specific host address, or a subnet designation.

The parameters of allow and deny can be a full absolute IP address, a partial IP address with an assumed mask, or an IP address with a mask. The assumed mask is 255.255.0.0 or 255.255.255.0. A zero in any field of the IP address means wild card. At this time, only subnet masks 255.255.0.0 and 255.255.255.0 have any meaning. A zero in any field of the IP address means wild card.

Correct use is to first deny everything via deny 0.0.0.0 and then one at a time allow subnets and/or specific IP addresses that exist at the site or EOC.

An address match refers to the client computer's IP address. If the client IP address Boolean-anded with the IP mask equals the IP address in the allow or deny directive, the match is set TRUE. If they are not equal then FALSE.

The following example allows access by all IP addresses on the PNL-Net, except for workstations wd_millard and merlin. Access by addresses on the PNL-Remote subnet (remote dial-in) are also allowed. The entire world outside PNL-Net and PNL-Remote are denied access.

```
[SITE PNL]
[ACCESS]
deny  0.0.0.0        # deny world
allow 130.20.0.0     # allow pnl-net...
deny  130.20.92.40   # deny wd_millard
deny  130.20.76.40   # deny merlin
[END of ACCESS]
[END of PNL]
```

4.2.4.2 HOST Block

The format of a HOST block declaration is

[HOST host1 host2 host3 ...]

where: host1 host2 is a list of one or more host names.

The HOST block is a conditional block which is compiled only if the server host, on which the command server daemon cmdservd is executing, is contained in the list of permitted hosts, i.e., the HOST block parameter list.

The following example defines the site to be PNNL, only if the name of the command server host is virus, locusts, temblor, or mirage. The example code fragment also sets up access for the site.

```
[HOST    virus locusts temblor mirage]
site     PNNL          # site name is PNNL
[END]
[SITE PNNL]
[ACCESS]
deny     0.0.0.0       # deny whole world
allow    130.20.92.0    # allow isb1-400-pod subnet
allow    130.20.194.0  # allow pnl-femis-1 subnet
allow    130.20.210.0  # allow pnl-femis-2 subnet
allow    130.20.226.0  # allow pnl-femis-3 subnet
allow    130.20.242.0   # allow pnl-femis-4 subnet
[END]
[END]
```

4.2.4.3 SITE Block

The format of a SITE block declaration is

[SITE site1 site2 ...]

where: site1 site2 is a list of one or more site names.

The SITE block is a conditional block that is compiled only if the server host, on which the command server daemon cmdservd is executing, is within one of the sites listed. The specific site is determined by the site directive.

In the following example, the ENTRY definitions are compiled only of the local host is in one of the named sites: PNNL, TEAD, and UMDA.

```
[SITE PNNL TEAD UMDA]
[ENTRY import]
...
[END]
[ENTRY execute]
...
[END]
[END]
```

4.2.4.4 ALL Block

The command server configuration file syntax rules require that all directives be contained inside of a block. Thus, a directive cannot be placed at the outer most level, as only blocks are allowed at that level.

In most cases, directives are not needed except inside blocks. However, there are special cases where placing a directive at the outer most block is necessary. The ALL block effectively allows that case. The ALL block is like a conditional block that is always TRUE. It might be used where a HOST or SITE block would be used, however the ALL block always compiles.

One special case that requires an ALL block is definition of global environment variables. Consider the following example.

```
[ALL]
environment DATABASE fi7
[END]
[HOST virus]
environment DATABASE fi6
[END]
```

In the example above, environment database is first defined to be fi7, all the time. Then if the host is virus, DATABASE is redefined to be fi6.

4.2.4.5 ENTRY Block

An ENTRY block defines a block of code that is used in the command server to set up the execution of a child subprocess. The command, script, or executable to be spawned can be a compiled program, a Bourne script, a C Shell script, or a PERL script.

The executable directive tells the command server where to find the entry's application file. Other directives set up arguments, parameters, and data being passed to the application.

The directive types permitted within an ENTRY block are as follows:

executable, directory, password, outfile, errfile, argument, environment, file, put, allow, and deny.

The parameter in the ENTRY statement is the entry name, which the command server matches with the parameter in a run command message from a client. See *cmdservd(1)* man page. Example:

```
<op:COMMAND|ac:run entry-name|...>
```

4.2.5 Directive Syntax and Semantics

In the command server configuration language, blocks define the structure of a configuration program, and directives define actions to be executed at some point.

Directives are coded on a single line, which does not begin with the [(left bracket) or # (comment) character. Generally, a directive consists of the directive type name, followed by an optional format statement, followed by one or more parameters.

Directives utilize a format string which appears much like the format strings of the C programming language. In this language, only the %s conversion type is valid, i.e., %d %x %u are not supported and, if included in a format, produce an error. Any number of %s conversions can appear in a format string. This is the way in which data from the client program is passed on to the application.

The parameters in a directive statement can be a simple string or the name of an environment variable. Environment names utilized get their values from the COMMAND:run messages from a client. In the example below, variables A, B, and C get values 1, 73, and 88X. All values are string values. Example:

```
<op:COMMAND|ac:run x|ev:A=1|B=73|C=88X|...>
```

Following is a table of directives in the command server language:

Directive	Purpose
site	Define the name of a site
executable	Define name of executable file
directory	Define default directory
password	Define password
outfile	Name the stdout file
errfile	Name the stderr file
argument	Specify a command line argument
environment	Specify an environment variable
file	Open and write a file
put	Put record into opened file
allow	Allow access by client
deny	Deny access by client

Three methods have been provided in the command server configuration language for copying input parameters to the application: argument, environment, and file/put. Argument generates an application command line argument. Environment creates an environment variable that then gets duplicated in the application. File and put create a file that can be read by the application.

4.2.5.1 Site Directive

The site directive defines the name of the site. This site name is then utilized in SITE blocks to conditionalize other blocks.

The site directive is only valid inside a HOST block. Example:

```
#
[HOST virus locusts temblor mirage]
site  PNL
[END]
#
[HOST cemsun tcemsun]
site  UTAH
[END]
```

```
#
[SITE PNL]
environment DATAPATH /files3/home/femis/data/pnl/
[END]
[SITE UTAH]
environment DATAPATH /files1/home/femis/data/utah/
[END]
#
[ENTRY xyz]
...
argument %s DATAPATH
[END]
```

Note: The same thing could be accomplished by using only the HOST block. However, SITE provides a convenient shorthand way to group a list of hosts that exist at the different CSEPP sites.

In the example above, the environment variable DATAPATH is changed depending on site value. Placing the definition of DATAPATH outside the ENTRY blocks helps to decrease the amount of configuration file code necessary.

4.2.5.2 Executable Directive

The executable directive provides the command server daemon with the executable file name. Possible formats are

```
executable file-name
executable format parameter-list
```

where file-name is an absolute. Only string data type is supported—no integer or floating data.

Format is a cmdserv allowed format (see above). Parameter list is a list of internal environment variable names. The number of environments in the list must match the number of %s designators in the format string.

The executable directive requires that the environment variables used to generate the file name must be internal only. For this directive, external (client) environments are not allowed. The command server daemon does not allow the client to override the value of a previously specified environment if that environment is then used in the name of an executable, which would constitute a significant security hole. Examples:

```
executable /home/femis/bin/import.sh

environment EXEPATH /home/femis/bin/esim/
executable  %s/import.sh  EXEPATH
```

In the examples above, the first example is valid because it is static and does not involve environments. The second example also is valid, provided the client does not override the value of environment EXEPATH.

4.2.5.3 Directory Directive

The directory directive provides the command server daemon with the path to use for current directory prior to running the application. See *chdir(2)* man page. Possible formats are

```
directory path-name
directory format parameter-list
```

where path-name is an absolute. Only string data type is supported—no integer or floating data.

Format is a cmdserv allowed format (see above). Parameter-list is a list of environment variable names, which may be internal and/or external (client generated). The number of environments in the list must match the number of %s designators in the format string.

If cmdservd can not set directory to the specified path, it returns an error message to the client, and does not run the application.

4.2.5.4 Password Directive

The password directive provides the command server daemon with the password to use for this application. The password string can be blank. If the password directive is omitted, it is assumed to be blank. A blank password means that password checking is not performed in cmdservd prior to running the application. Possible formats are

```
password password-string
password format parameter-list
```

where password-string is the full password specification. Only string data type is supported—no integer or floating data.

Format is a cmdserv allowed format (see above). Parameter-list is a list of internal environment variable names. The number of environments in the list must match the number of %s designators in the format string.

The password directive requires that the environment variables used to produce the password string must be internal only. For this directive, external (client) environments are not allowed. The command server daemon does not allow the client to override the value of a previously specified environment if that environment is then used in a password directive, which would constitute a significant security hole because the client could specify its own password.

If the password directive specifies a non-blank string, cmdservd then requires the client to send a password string in the COMMAND message. That password must match the one generated in the password directive. If a match is not realized, cmdservd returns an error message to the client, and does not run the application. Examples:

```
password georgewashington

password Elisabeth-2

environment SPORT Baseball
environment TEAM SeattleMariners
environment PLAYER KenGriffyJr
password %s-%s TEAM PLAYER
```

The first and second examples specify valid passwords because they are static and do not involve any environments. The third example also is valid, provided the client does not override the value of environments TEAM or PLAYER.

4.2.5.5 Outfile Directive

The outfile directive tells the command server daemon the file name of where to write the application's standard output. If no /path is included in the outfile directive, the file will be written to the default directory.

If outfile and errfile specify the same string, only one file is created and stdout and stderr point to the same descriptor.

Possible formats are

```
outfile file-name
outfile format parameter-list
```

where file-name is a full or partial file specification. Only string data type is supported—no integer or floating data.

Format is a cmdserv allowed format (see above). Parameter-list is a list of environment variable names, which may be internal and/or external (client generated). The number of environments in the list must match the number of %s designators in the format string.

4.2.5.6 Errfile Directive

The errfile directive tells the command server daemon the file name of where to write the application's standard error. If no /path is included in the errfile directive, the file will be written to the default directory.

If errfile and outfile specify the same string, only one file is created and stdout and stderr point to the same descriptor.

Possible formats are

```
errfile file-name
errfile format parameter-list
```

where file-name is a full or partial file specification. Only string data type is supported—no integer or floating data.

Format is a cmdserv allowed format (see above). Parameter-list is a list of environment variable names, which may be internal and/or external (client generated). The number of environments in the list must match the number of %s designators in the format string.

4.2.5.7 Argument Directive

The argument directive tells cmdservd to copy the directive parameter(s) to the application's command line arguments in the order given. See *execve(2)* man page. Possible formats

```
argument argument-string
argument format parameter-list
```

where argument-string is one full argument in string format. Only string data type is supported—no integer or floating data.

Format is a cmdserv allowed format (see above). Parameter-list is a list of environment variable names, which may be internal and/or external (client generated). The number of environments in the list must match the number of %s designators in the format string. Examples:

```
argument -x
argument inputfile.dat
argument %s-%s  TEAM  PLAYER
```

4.2.5.8 Environment Directive

An environment directive tells cmdservd to define an environment variable in cmdservd process space. See *setenv(1)* and *putenv(3)* man pages. Environment variables can be used to generate the other application attributes, i.e., arguments, directory, file names. Environment variables also are inherited by the child process, and thus can be used to transmit data to the application.

In some cases, this method of transmitting input parameters to the child has an advantage over using the argument directive. Those situations include when security is an issue, because using UNIX can make arguments visible via the ps command.

Possible formats are

```
environment env-name env-value-string
environment env-name format parameter-list
```

where env-name is the environment variable name. Env-value string is the environment variable value. Only string data type is supported—no integer or floating data.

Format is a cmdserv allowed format (see above). Parameter-list is a list of environment variable names, which may be internal and/or external (client generated). The number of environments in the list must match the number of %s designators in the format string.

Note: Environment variables subsequently used in executable or password directives, which are affected by the client message, are not allowed. The command server daemon terminates the entry and does not run the specific application, because to do so would constitute a security hole. In other words, the client can not specify its own password nor its own executable file. Only the configuration file can do that.

Examples:

```
environment OPTION -x
environment SPORT BBall
environment TEAM ChicagoBulls
environment PLAYER Jordan
environment TEAMPLAYER %s.%s TEAM PLAYER
```

4.2.5.9 File Directive

The file directive instructs cmdservd to create and open a new file to receive records. Records are written to the file via the put directive.

Possible formats are

```
file file-name
file format parameter-list
```

where file-name is either a full or partial file specification. If a relative file name, the default directory is utilized as the starting point.

Format is a cmdserv allowed format (see above). Parameter-list is a list of environment variable names, which may be internal and/or external (client generated). The number of environments in the list must match the number of %s designators in the format string. Examples:

```
file /home/femis/user/evlog/10000745/e0/
file /home/femis/user/evlog/%s/e%s/pf CASE EXER
```

In the first example, the file directive uses a full path specification involving no variables. The second example utilizes two variables CASE and EXER, assumed to be sent by the client.

A command server configuration file entry can utilize multiple file directives, in which case multiple files are created.

4.2.5.10 Put Directive

The put directive instructs cmdservd to copy one record into the file created and opened by the most recent file directive.

Possible formats are

```
put record-text
put format parameter-list
```

where record-text is the actual and full record text to be copied into the currently opened file.

Format is a cmdserv allowed format (see above). Parameter-list is a list of environment variable names, which may be internal and/or external (client generated). The number of environments in the list must match the number of %s designators in the format string. Examples:

```
put "The quick brown fox jumped over the lazy dog."
put %s-%s CASE EXER

environment ANIMAL elephant.
put "The quick brown fox jumped over the %s." ANIMAL
```

The first example copies a fixed static string into the file. The second utilizes a format string and two environment variables. The third example uses a quoted string as the format and one environment variable. The ANIMAL value could be provided in a message from the client.

4.2.5.11 Allow Directive

A description of the allow directive is also included in ACCESS block documentation. Combinations of allow and deny can be used in ACCESS and ENTRY blocks to describe the permitted users of the command server.

Syntax of the allow directive is the keyword allow, followed by an IP address or subnet, followed by an optional subnet mask, followed by an optional comment.

Format of IP address and subnet mask currently is four decimal numbers, in the range 0-255, separated by decimal point. Allowed IP address elements are 0-255.

Allowed IP mask elements are 0, 128, 192, 224, 240, 248, 252, 254, and 255. Subnet mask must be in the format 255...XXX.0..., where 255 can appear one, two or three times; 0 can appear one, two, or three times; and XXX (not 0 or 255) can appear only one time. Examples:

```
allow 0.0.0.0                    # world
allow 130.20.0.0      255.255.0.0    # pnl net
allow 192.101.108.0   255.255.255.0  # pnl-remote
allow 130.20.92.131              # workstation
allow 201.8.44.64 255 255.255.224    # subnet
```

4.2.5.12 Deny Directive

A description of the deny directive is included in the ACCESS block documentation. Combinations of allow and deny can be used in ACCESS and ENTRY blocks to describe the permitted users of the command server.

Syntax of the deny directive is the keyword allow, followed by an IP address or subnet, followed by a subnet mask, followed by optional comments.

Format of IP address and subnet mask currently is four decimal numbers, in the range 0-255, separated by decimal point. Allowed IP address elements are 0-255.

Allowed IP mask elements are 0, 128, 192, 224, 240, 248, 252, 254, and 255. Subnet mask must be in the format 255...XXX.0..., where 255 can appear one, two or three times; 0 can appear one, two, or three times; and XXX (not 0 or 255) can appear only one time. Examples:

```
deny 0.0.0.0                     # world
deny 196.104.8.0                 # subnet
deny 130.20.92.87                # workstation
deny 201.8.44.32  255.255.255.224  # subnet
deny 201.8.44.96  255.255.255.224  # subnet
```

4.3 cmdserv – FEMIS Command Server Test Client (UNIX)

4.3.1 Synopsis

cmdserv [-v] [-h] [-D] [-u] [[IPaddr] | [hostname]] [port]

4.3.2 Availability

Program cmdserv is a test client for use with the FEMIS command server daemon cmdservd. The command server, test client, and related files are delivered in the FEMIS distribution tar file on magnetic tape or CD. The default locations for these files are /home/femis/bin and /home/femis/etc on the FEMIS UNIX data server.

4.3.3 Description

FEMIS utilizes remote command servers, executing on a UNIX host computer in order that PC workstation users can launch large mathematical model/simulation codes, which on the PCs either could not be run at all or would require an unreasonable amount of time and resources. These include the Evacuation SIMulation (ESIM), a module in the Oak Ridge Evacuation Modeling System (OREMS).

The command service consists of a client and server. The client runs on a Windows NT workstation. The server runs on UNIX and is capable of spawning processes at the request of a remote client.

This program is a client for use on the UNIX platform. Its purpose is mainly for testing the command server, for testing of new configuration file scripts, and for testing executables.

4.3.4 Options

The command server test client -v option produces a listing of current version information. Example:

```
virus% cmdserv -v
cmdserv version 1.0 - Wed Feb 14 14:41:00 PST 1996
```

The cmdserv -h option produces a help listing:

```
virus% cmdserv  -h
usage: cmdserv  [-hvD] [IPaddr | host] [port]
       -v       : display version information
       -h       : display help messages
       -D       : use unregistered service port (9015)
       Ipaddr   : host IP address, e.g., 130.20.92.87
       host     : server's host name, e.g., cemsun
       port     : protocol or service port, e.g., 9015
```

The cmdserv -D option turns on diagnostics.

Normally, the destination port is 9015, the standard service port for the FEMIS command server. Certain testing activities may require changing the cmdserv port number, thus the option to place it on the command line.

The destination host must be specified either as an IP address, or as a host name. One or the other must be specified, but not both. The local host can be designated as the command server daemon by including minus sign (-) in place of the IP address or host name. Examples:

```
virus% cmdserv locusts
virus% cmdserv virus
cemsun% cmdserv tcemsun
cemsun% cmdserv cemsun
virus% cmdserv -
```

```
virus% cmdserv 130.20.92.87
locusts% cmdserv 130.20.28.43
```

4.3.5 Installation

See the *cmdservd(1)* man page.

4.3.6 Protocol

See the *cmdservd(1)* man page.

4.3.7 Operation

Run the command service test client by entering cmdserv. Cmdserv first tries to connect with the command server daemon, cmdservd. Generally, any I/O error during execution of the test client will cause it to terminate. The possible errors during client operation are

cmdserv: create socket failed: PERROR
- Call to socket() library function to create a socket failed with the error indicated.

cmdserv: convert IP address failed: PERROR
- Call to inet_addr() library function failed with the error indicated.

cmdserv: HOST - unknown host: PERROR
- Call to gethostbyname() library function failed with the indicated error.

cmdserv: HOST-OR-IP - connect failed: PERROR
- The connect() library function call failed because of the indicated error.

cmdserv: HOST-OR-IP - can't get socket info: PERROR
- Call to getsockname() library function failed because of the indicated error.

cmdserv: read failed: PERROR
- Call to recv() library function to receive a message on a socket failed with the error indicated.

cmdserv: send failed: PERROR
- Call to send() library function to transmit a message on a socket failed with the error indicated.

where HOST-OR-IP will be either the destination host name or the destination IP address depending on how the command line was entered. And PERROR represents an error message returned from perror().

Once cmdserv receives control from the shell, it opens a connection to the specified destination host, and prompts for an action.

Action

Prior to entering anything, wait for the server and client hello messages to be exchanged. Cmdserv displays two to three messages. Example:

Received

```
<op:MISCINFO|
   program argv   :  cmdservd|
   program argc   :  1|
   current dir    :  /files0/home/larryg/femis/command/log|
   config file    :  \LNull\R|
   daemon uid     :  1033|
   getpeemame     :  clen : 16|
   getpeemame     :  gprc : 0|
   client port    :  2377|
   client host    :  hattrick.pnl.gov|
   client Ipadd   :  130.20.92.87|
   hwid number    :  82145C57|
   server key     :  \Lnull\R|
   client key     :  \Lnull\R|
   process id     :  10332|
   parent id      :  146>
```

Received

```
<op:SVRHELLO|F2BBE247|********|********>
```

Sending

```
<op:CLIHELLO|********|********|mo:alert test >
```

Action

At this point, enter one of the following:

```
run X      : runs entry X from configuration file
status     : returns status of current application
kill       : kills the current application
```

After entering run X, cmdserv prompts for a password.

Password

Either enter the password required by the configuration file or just enter return if none is required. Also see the configuration file *cmdserv.conf(5)* man page.

Cmdserv next prompts for any number of parameters. Parameters must be of the form VARIABLE=VALUE, where VARIABLE is the name of a variable in the command server, and VALUE is the value to be assigned.

> **Note:** All values are string values. Numeric, integer, or floating point data is not supported in this implementation.

Once all parameters have been entered, type return or ^D.

As soon as the command server processes the command and starts the application, it sends a message back to cmdserv, which is displayed:

Received

<op:REPLY|rc:active TIMESTAMP PROCESS>

where TIMESTAMP is a 10 character time stamp, e.g., 9602071334, and PROCESS is the PID of the child process.

While the application is executing, entering status returns status of the application process. Once the application has terminated, the command server sends an alert message and cmdserv displays:

Received

<op:ALERT|rc:finish TIMESTAMP PROCESS>

where TIMESTAMP and PROCESS are the same as above.

Now enter another command or exit via ^C or ^D.

4.3.8 Messages

Any of the possible command server daemon (cmdservd) error messages and reply messages can be received in the test client and thus be displayed on its standard output. See the *cmdservd(1)* man page.

4.3.9 Configuration File

See the *cmdserv.conf(5)* man page.

4.3.10 Service Port and Name

The cmdserv service port number currently is 9015. The short name is femis-cmdserv or fxcmdserv.

4.3.11 Files

Files utilized during the installation and execution of the FEMIS command server include

/home/femis/bin/cmdservd	daemon executable
/home/femis/etc/cmdserv.conf	configuration file
/home/femis/bin/cmdserv	test client (UNIX)
/etc/services	service port numbers
/etc/inetd.conf	internet daemon config

5.0 FEMIS Met Application

The FEMIS Met (meteorological) application can obtain Met data in two ways. Met data is transferred from EMIS to FEMIS using the FEMIS Data Exchange Interface (DEI). The second method is to use the FEMIS Met Injection tool.

5.1 Met Input Using the FEMIS DEI

The FEMIS DEI automatically acquires operational Met data from EMIS and places it into the FEMIS Met tables. The DEI can also be configured to send a copy of the operational Met information into a specified FEMIS exercise. The option to store a copy of operational Met data in a selected exercise in not enabled when the DEI is installed at a site. This reduces the amount of disk space needed to store Met data and allows the site administrator to only get a copy of operational Met data when it is appropriate, such as during an exercise.

5.2 Met Input via the FEMIS Met Injector

FEMIS has a stand-alone Met Injection tool that allows a privileged user to enter operational and/or exercise Met values into the FEMIS Met tables. This tool is expected to be used by a controller to input the specific Met values needed an exercise. A description of how this tool works is available in the FEMIS Help.

6.0 FEMIS Contact Daemon

All network communication servers in FEMIS utilize the standard registered service port for making contact between all clients and all servers. By registered, we mean that the FEMIS project has requested registration for and received notification of a single TCP/IP service port from the Internet Assigned Number Authority (IANA). The name registered and port assigned are femis 1776.

To implement the registered FEMIS service port on a server, the line femis 1776 has been added to the /etc/services file. Doing this tells *inetd* that any incoming connection request directed to port 1776 is intended for one of the four FEMIS server daemons: met, notification, command, or monitor.

Upon receiving a connection request on port femis 1776, *inetd* forks and executes the femisd program, the FEMIS contact protocol daemon. The only job of femisd is to figure out which of the four service protocols the client application needs. This is done by reading a single message from the client. That message contains the requested protocol name and a list of parameters. femisd then executes the correct protocol handler and passes control to it. All communication with the protocol handler then takes place over the socket established in *inetd*.

6.1 Message Format

The message format which clients utilize to communicate with femisd is <pro:P|env:E|arg:A> where P is the protocol name, E is an environment specification, and A is an argument specification for the process to be executed. The femisd message can contain any number of environment and argument messages. Environment specifications are used to modify the process environment prior to calling the protocol server. Arguments are passed to the protocol server on the command line.

6.2 Configuration File

This section discusses the format of the femisd configuration file.

The contact daemon configuration file default location is /home/femis/etc/femisd.conf. This can be over-ridden by the -conf <file> command line option.

Any line starting with a # is a comment line.

A line debuglevel NUMBER specifies the level of debug output in the log file /home/femis/log/femisd.log. NUMBER is 0, 1, 2, or 3. The value 0 is the least verbose. The value 3 is the most verbose. Use the higher values of debuglevel only for debugging and diagnostic. Using debuglevel 3 fills up the disk quickly.

A line PROTOCOL EXECUTABLE OPTIONS is the way to specify an interface to a protocol handler. Presently there are protocol handlers for command server, FEMIS monitor daemon, and notification server. The names are cmdservd, femismond, and fxnotify.

PROTOCOL are numbers usually in the range 9000-9999. These are not port numbers. The port number is always 1776. Protocol numbers are the same numbers as were port numbers in all previous FEMIS releases. Thus, continuity in command line formats has been retained, greatly simplifying implementation. Example: normal notification protocol numbers are in the range 9020-9034.

EXECUTABLE is the full executable path/name to the protocol handler. Example: normal notification protocol handler is /home/femis/bin/fxnotify.

OPTIONS is a list of special command line switches. They are

OPTIONS string < %N -- %P %C %J -H %H > is currently included on every line in the femisd configuration file. These specify program name, protocol number, client host, client port number, and home directory.

Option %N is substituted for by the femisd program name string.

Option %V is substituted for by the femisd version number string.

Option %H is substituted for by the home directory string.

Option %U is substituted for by the UID code of the femisd process.

Option %A is substituted for by the architecture string from uname.

Option %M is substituted for by the machine type string from uname.

Option %S is substituted for by the host name of the server.

Option %C is substituted for by the host name of the client.

Option %I is substituted for by the IP address of the client.

Option %J is substituted for by the client port number of the client.

Option %R is substituted for by the process id number of the FEMIS process.

Option %P is substituted for by the protocol name part of the message.

Option %D is substituted for by the current date in YYYYMMDD format.

Option %T is substituted for by the current time in HHMMSS format.

Option %F is substituted for by the full time stamp in YYYYMMDDHHMMSS format.

Option %E(V) is substituted for by the value of environment variable is V.

Note: The %D and %F format are both Year 2000 compliant. The purpose of these and other options is for creating unique and different log file names from parameters readily available to the femisd program.

7.0 FEMIS Data Exchange Interface (DEI)

The FEMIS/EMIS Data Exchange Interface (DEI) system is used to support the transfer of data from EMIS to FEMIS.

The FEMIS/EMIS Data Exchange Interface system consists of one main program (femisdei) for processing data sent from EMIS and a utility program (fprofdei) for maintaining the encrypted password file for File Transfer Protocol (FTP). Both programs run on the FEMIS onpost UNIX computer, the former usually as a background process.

From the EMIS perspective, IBS and FEMIS are essentially indistinguishable. The files are sent from EMIS via FTP to an Internet Protocol (IP) address and some files come back from them in a particular directory. At most, two changes need to be made to EMIS, both on the UNIX computer.

1. The setup.ini file may need to be changed to specify the EMIS UNIX user account for incoming files (and the account created if it does not exist). The recommendation, however, is to continue using the current account used for communicating with IBS.

2. The template file in the EMIS UNIX user's home directory needs to be changed to point to the new IP address, FEMIS UNIX user account, and password.

EMIS will then communicate with FEMIS instead of IBS.

7.1 Software and Hardware Components

7.1.1 Software Components

- FEMIS/EMIS Data Exchange Interface program – femisdei
- FEMIS/EMIS FTP Profile Manager – fprofdei

7.1.2 Hardware Components

- FEMIS onpost UNIX computer
- EMIS computers (PC and UNIX)

7.2 Program Detail – femisdei

The femisdei program processes files received from EMIS in a manner similar to the EVENT program in IBS. It is a PRO*C program which connects to an Oracle database and loads data into various tables. The program has three distinct phases of operation: startup, processing loop, and shutdown.

7.2.1 Startup Phase

During the startup phase, the program sets some default configuration items, processes the configuration file and overrides the default setup, and then processes the command line options which override all previous settings. If everything is working so far, it connects to the Oracle database. If able to connect, it then checks to see if the specified FEMIS exercise exists. If not, the program displays a warning message and continues. Then, if you want it to run as a background process (the -clone command line option or the CLONE configuration file option) like it normally does, it moves itself into background.

7.2.2 Processing Loop Phase

Next, the program begins the processing loop, where it waits for a transfer list file, xferlist.dat, to appear in the /home/femx directory. When the file appears, FEMIS DEI moves the EMIS files to the "from" directory, reads the header, and determines whether the accompanying files are real or exercise data. It reads and processes the entries one file at a time, sends notifications of new data to the FEMIS Notification server via the fev client, and sends a KEY.DAT file back to EMIS using FTP to acknowledge receipt of the files. Then it waits for another transfer list file.

Generically, processing a data file consists of

1. Reading the file header
2. Adding an entry to the FEMIS journal that the file was received from EMIS
3. Reading the data in the file
4. Converting the data into FEMIS terms
5. Putting the results into the Oracle tables
6. Adding entries to the FEMIS journal that the file was successfully processed
7. Adding entries to the notification list
8. Adding an entry to the acknowledgment key list
9 Sending the acknowledgment back to EMIS.

EMIS can send many types of files, but femisdei only loads the data in a few of them. These are NOTIFY.DAT, D2INPnnn.DAT, WORKPLAN.DAT, and WEATHER.DAT. A KEY.DAT file with a Please Echo key or a PAR key will also be processed properly. All files from EMIS will be acknowledged, though the files that femisdei ignores will always be said to be OK (DATA_OK). The other files may or may not be OK based on the contents of each file.

NOTIFY.DAT: If the transfer includes a Notification file, femisdei processes it first. It reads the entire file and then determines whether this is a new event, an update to an existing event, or closes one or all EMIS events.

To determine if one or more EMIS events are to be closed, the END EVENT Classification is used to close the specified event, and END ALL OPER EVENTS or END ALL EXER EVENTS is used to close all EMIS events. If only closing a single event, then the event in FEMIS with the same EMIS Event ID is ended. Otherwise all EMIS events in FEMIS in the proper mode (operations or exercise #n) are ended.

The new versus update notification is determined by looking at the EMIS Event ID and the Notification Reason field. If there is an event in FEMIS with the same EMIS Event ID, then this is an update. Otherwise, it is a new event. Then get the current operational D2PC case from the Local Config table. Next, add a record for the event to the CSEPP Accident table. Then, if it is an update notification, change the Chemical Accident or Incident (CAI) Status Code flag for all previous records for that event, leaving just the new record as the current one.

D2INPnnn.DAT: After processing the notification file, femisdei processes the D2PC input file, if sent. First, it calculates the D2PC case number by extracting it from the name of the file (the nnn). Then it renumbers or deletes any D2PC cases in the database which have the same D2PC case number. (The first available number greater than 1000 is used). If the FEMIS Work Plan points to an old D2PC case with that number, the program makes it point to the new D2PC case. Then it adds an empty record in the database for the new D2PC case. Next, it processes the file, loading the values into the various D2PC tables. If the D2PC case is a real one (not Reference or What-If), then it updates the Local Config table to point to the new D2PC case. (In other words, the D2PC case sent from EMIS becomes the current operational onpost case in FEMIS.) Next it copies the Operations record in the Local Config table to the OperOnpost record. Then it updates the SendOffpost flag in the Val List table. Finally, it adds an entry to the Case Management table for the new D2PC case.

WORKPLAN.DAT: For each activity in the WORKPLAN.DAT file, FEMIS DEI reads the data from the file and adds an activity record to the FEMIS database. A number of the fields in this new activity record will be missing information because that information is not supplied by EMIS. A Local ID/MCE **may be created.** Local ID/MCEs are based on D2PC source term information, but the WORKPLAN.DAT file only specifies agent and munition. If no Local ID/MCE exists with the specified agent and munition, then a new Local ID/MCE will be created. When it is done processing the file, it sets the new Work Plan as the operational Work Plan.

WEATHER.DAT: For each entry in the Weather file, it reads the record, finds the tower name associated with that tower ID, makes all current meteorological records for that tower not current, and adds the new record, making it current.

Note: The current date/time is used, not the date/time the reading was taken, since the latter is not really supplied by EMIS.

7.2.3 Shutdown Phase

The final phase, shutdown, usually will not occur. In fact, it can only occur if you run femisdei in One Pass mode, if you "kill" it with the kill file, femisdei.kil, if Oracle goes down, or if femisdei crashes. The kill file causes femisdei to shutdown nicely, committing all outstanding database updates and disconnecting from Oracle. While you can use the UNIX kill -9 command, it simply stops femisdei dead in its tracks and does not force database commits or the database disconnect to occur–two things could happen that you do not want to happen. First, not all the data from EMIS will be saved in the Oracle database. Second, the Oracle connection **may not** immediately go away. This could prevent femisdei or other programs that access Oracle from getting a connection. Therefore, to stop the femisdei program, **always** use the femisdei -kill option.

7.3 Program Detail - fprofdei

The fprofdei C program is used to maintain the FTP profile file. This file is usually named /home/femis/etc/femisdei.prf. It contains the hostname, username, and encrypted password for the EMIS UNIX computer to which femisdei will send acknowledgment files via FTP. It is analogous to the template file that EMIS uses to transfer files to IBS or FEMIS.

7.4 Configuring the Programs

The FEMIS UNIX Installation scripts configure DEI automatically, you should not need to do anything. However, if you do need to configure the programs, the following procedures detail the configuration procedures for the femisdei and fprofdei programs.

7.4.1 Configuration – femisdei

The femisdei program requires the following directory structure:

```
/home/femis/bin       - directory for executables
/home/femis/etc       - configuration files
/home/femis/log       - log files
/home/femx            - incoming files from EMIS
/home/femx/dei/send   - outgoing files to EMIS
/home/femx/dei/from   - saved files from EMIS
```

Note: ALL of the above directories are configurable, but this is the recommended setup.

The UNIX programs and support files are in the indicated locations, which is where they are placed when loaded from tape.

```
/home/femis/bin/femisdei      - executable file
/home/femis/bin/fprofdei      - executable file
/home/femis/etc/femisdei.cfg  - configuration file
/home/femis/etc/femisdei.prf  - configuration file
```

7.4.1.1 femisdei UNIX User Account

femisdei requires a UNIX user account for receiving files from EMIS. The recommended setup is:

- Username is femx.
- Home directory is /home/femx.

- Directory structure is

  /home/femx/
  /home/femx/dei/from
  /home/femx/dei/send

- The femisdei program must be able to read and write to all of the directories.

7.4.1.2 femisdei FTP Profile File

The femisdei program requires an FTP profile file, usually named /home/femis/etc/femisdei.prf. It is maintained with the fprofdei utility, which you should refer to for more information.

7.4.1.3 femisdei Configuration File

The femisdei program requires a configuration file, usually named /home/femis/etc/femisdei.cfg. This file is automatically configured during installation, but you may need to change it later. Comments lines (blank or beginning with #) are ignored. Refer to the sample configuration file in Table 7-1 at the end of this section.

PATH (recommend /home/femis/bin:/usr/bin): $ORACLE_HOME/bin
UNIX PATH environment variable. Should be set correctly before femisdei starts.

ORACLE_SID
UNIX Oracle environment variable. This variable should be set correctly before femisdei starts.

ORACLE_HOME
UNIX Oracle environment variable. Should be set correctly before femisdei starts.

ORACLE_BASE
UNIX Oracle environment variable. Should be set correctly before femisdei starts.

DEIPATH (recommend /home/femx/dei/)
Top-level directory under which the from and send directories must be located and where femisdei puts files from EMIS or files it sends to EMIS. Make sure to include the slash (/) at the end. It can be overridden with the -dei <path> command line option.

EMISPATH (recommend /home/femx/)
Home directory of the femx user, and directory where EMIS put its files. Make sure to include the slash (/) at the end. It can be overridden with the -ep <path> command line option.

PROFILEFILE (recommend /home/femis/etc/femisdei.prf)

Name of the FTP profile file which contains the hostname, username, and encrypted password of the EMIS account to which femisdei will FTP files. It can be overridden with the -pf <fn> command line option.

HALTFILE (recommend /home/femis/log/femisdei.hlt)

Name of the halt file which will cause femisdei to halt. When the file disappears, femisdei will continue processing. This is also the file that gets created with the femisdei -halt command.

Note: If the file exists when femisdei starts, it will halt.

KILLFILE (recommend /home/femis/log/femisdei.kil)

Name of the kill file that will cause femisdei to exit gracefully. This is also the file that gets created with the femisdei -kill command.

Note: If the file exists when femisdei starts, it will immediately exit, deleting this file.

LOGFILE (recommend /home/femis/log/femisdei.log)

Name of the output log file. It can be overridden with the -log <fn> or -nolog command line options.

FEVHOST, FEVPORT

Name of the FEMIS UNIX onpost computer and port number for use by the fev client for sending notifications of new data to the FEMIS Visual Basic applications. It can be overridden with the -fev <host> <port> command line option.

FTPHOST, FTPUSER, FTPPATH (recommend ./)

Name of the EMIS UNIX computer, username, and path where femisdei will FTP files. It can be overridden with the -ftp <host> <user> <path> command line option.

EXERCISE

Exercise number into which exercise data from EMIS will be loaded. The exercise number does not necessarily have to be a valid exercise in FEMIS–the data will be loaded anyway. It can be overridden with the -exercise <n> command line option.

SLEEP (recommend 1)

The time interval that femisdei waits between checking for the xferlist.dat file from EMIS. It should not be more than 10 seconds. It can be overridden with the -sleep <seconds> command line option.

DAIINT (recommend 60)

The number of sleep intervals the femisdei should wait before checking for data acknowledgments to be forwarded to EMIS. The period of data acknowledgment checks may be calculated by multiplying the SLEEP and DAIINT values. For example, if the SLEEP parameter is set to 2 seconds and the DAIINT is set to 30, then data acknowledgments will be checked once every 2*30 = 60 seconds.

It can be overridden with the -daiint <number sleep intervals> command line option.

DEBUG (recommend NODEBUG)

The debug mode, which controls the detail of messages from femisdei. After you get femisdei running properly, you should run in nodebug mode, which just lists the name of each file from EMIS as it gets processed. Debug level 0 gives slightly more detailed messages, and debug level 2 gives very detailed messages, which would be useless to anyone but the developer. It can be overridden with the -debug, -debug 1, -debug 2, and -nodebug command line options.

CLONE (recommend CLONE)

Controls whether femisdei runs as a foreground or background process. For testing purposes, you may want to run it in foreground, but that means when you want to logout, the process will have to be killed. Normally, femisdei should be run as a background process. It can be overridden with the -clone and -noclone command line options.

CLEAN (recommend CLEAN)

Controls whether temporary files and files are deleted or left around. Both fev.csh and ftp.csh are temporary files created and executed from the /home/femx/dei/send directory. ftp.csh contains the password for the EMIS account, so the file should be deleted. That means that during normal operations, femisdei should clean temporary files. It can be overridden with the -clean and -noclean command line options.

SAVEEMIS (recommend NOSAVEEMIS)

Controls whether files from EMIS are saved by renaming them to include a time stamp, or whether they are simply deleted. It can be overridden with the -saveemis and -nosaveemis command line options. If there is a problem with the EMIS to FEMIS interface, then you should turn this option on. Otherwise, turn it off and run DEI with the -purge option to clean out the directory.

If you run DEI with the SAVEEMIS option turned on, then the from directory will actually include the date as part of its name, e.g., /home/femx/dei/from-1996-10-31. The send directory will be the same way. All files received from and sent to EMIS will be saved. However, the NOSAVEEMIS option saves just the last set of files from/to EMIS and does not include the date as part of the directory names. If you run DEI with the SAVEEMIS option, you should occasionally delete the old from and send directories or they will fill up the list.

DOTZ (recommend DOTZ)

Controls whether dates are converted from local time to GMT. It can be overridden with the -dotz or -nodotz command line options. There is no reason you should ever need to use the -nodotz option. It is only used for testing purposes.

KEEPD2 (recommend KEEPD2)

Controls whether real run D2PC cases from EMIS which have the same number as the new case are saved (renumbered) or deleted. It can be overridden with the -keepd2 or -nokeepd2 command line options. If you want to keep real run, every case that EMIS sends, then use the -keepd2 option, bearing in mind that it will eventually fill up the database.

KEEPWIFD2 (recommend NOKEEPWIFD2)

Controls whether what if D2PC cases from EMIS which have the same number as the new case are saved (renumbered) or deleted. It can be overridden with the -keepwifd2 or -nokeepwifd2 command line options. Since what if cases generally come from EMIS every fifteen minutes, it is highly recommended that you use the -nokeepwifd2 option to avoid filling up your database.

WIFREPRUN (recommend NOWIFREPRUN)

Controls whether what if cases can overwrite "real run" cases from EMIS which have the same number as the new case to be saved. It is highly recommended that you use NOWIFREPRUN to avoid having what if cases overwrite real run cases.

DUPMET (recommend NODUPMET)

Controls whether Met data is duplicated to both real and exercise mode as it arrives for processing. The DUPMET setting might be used if an EOC needs to simultaneously run an exercise and yet still have live Met in real mode. For the sake of conserving database space, it is recommended that this be set to NODUPMET unless an exercise is being run requiring Met data.

NEWLOG (recommend NEWLOG)

Controls whether log messages are written to a new log file (see LOGFILE) or appended to an existing one when you restart femisdei. It can be overridden with the -newlog or -nonewlog command line options.

7.4.2 Configuration – fprofdei

The fprofdei program requires no configuration.

7.5 Operation

The operating instructions for the femisdei and fprofdei programs are discussed in the following sections.

7.5.1 Operation – femisdei

First, a configuration file is required. If you do not specify one, the default is ./femisdei.cfg. If it does not exist, /home/femis/etc/femisdei.cfg is used. If that file does not exist, femisdei will not run. A properly setup configuration file means that femisdei can be run as follows:

```
% femisdei
```

However, even if the configuration file exists, femisdei may not run. When testing, you can override most of its settings with command line options. See Table 7-2, at the end of this section, for a list of femisdei command line options.

Note: femisdei is normally started automatically when the system boots from /etc/init.d/femis.

Note: femisdei should be manually restarted after any server time change.

7.5.2 Operation – fprofdei

The first step when running fprofdei is deciding where you are going to put the FTP profile file. If you do not specify the name of the file on the command line, it will create/modify the femisdei.prf file in your current directory. However, the recommended location is /home/femis/etc/femisdei.prf. If you put it elsewhere, you must modify the DEI configuration file, /home/femis/etc/femisdei.cfg.

Next, you need to know the hostname, username, and password of the EMIS UNIX account to which femisdei will FTP files. You can use the same account as used by IBS, which is specified in the file IEMIS$SYSF:POST_SYSTEM.DAT on the county VAX. The password in that file is not encrypted.

You are now ready to run fprofdei.

Note: fprofdei is automatically run during the FEMIS installation process by the FEMIS UNIX Installation script, which creates the appropriate .pr file.

Syntax : fprofdei [-f <profilefile>] <hostname> <username> [<password>]

where: <profilefile> = name of the profile file. If not specified, the default is ./femisdei.prf. The recommended name: /home/femis/etc/femisdei.prf.

where: <hostname> = name of the EMIS UNIX computer

where: <username> = username of the account on the EMIS UNIX computer

where: <password> = password of the account on the EMIS UNIX computer. If you do not specify it, you will be prompted.

Example:

fprofdei -f /home/femis/etc/femisdei.prf tadsun1 ibsxfer ibsx

The specified host, user, and password (encrypted) will be placed in the FTP profile file. If you run fprofdei more than once for the same host and user, it will replace the earlier entry with the new one.

While the FTP profile file can have multiple entries, the femisdei program only uses the one entry which corresponds to the EMIS host from which it receive files. It determines the EMIS host by extracting the name from the header of the transfer list file, xferlist.dat, which accompanies all files from EMIS.

7.6 DEI Troubleshooting

The troubleshooting instructions for the femisdei and fprofdei programs are discussed in the following sections.

7.6.1 Troubleshooting – femisdei

For femidei, make sure

- femis account is correct.
- femx account is correct.
- Oracle is accessible.

7.6.2 Troubleshooting – fprofdei

If DEI does not add an entry to the recommended FTP profile file, /home/femis/etc/femisdei.prf, check the following:

- If you used the -f option, you probably did not specify the correct file name.
- If you did not use the -f option, then you were probably not in the /home/femis/etc directory when you ran the program.

Table 7.1. Sample femisdei.cfg File

```
#
# $Id: femisdei.cfg,v 1.15 1998/05/14 18:12:52 femis Exp $
#=============================================================
# Purpose:
#   Configuration file for FEMISDEI.
#
#   For more information, see the FEMIS System Administration Guide.
#
#   Setup the following environment variables before running FEMISDEI.
#   ORACLE_SID
#   ORACLE_HOME
#   PATH
#   LD_LIBRARY_PATH
#=============================================================
#...Other settings
ORACLE_USER <db code>/<db passwd>
DEIPATH         /home/femx/dei/
EMISPATH        /home/femx/
PROFILEFILE     /home/femis/etc/femisdei.prf
HALTFILE        /home/femis/log/femisdei.hlt
KILLFILE        /home/femis/log/femisdei.kil
LOGFILE         /home/femis/log/femisdei.log
FEVHOST         temblor
FEVPORT         9021
FTPHOST         temblor
FTPUSER         emisx
FTPPATH         ./
EXERCISE        1
SLEEP           1
DAIINT          60

#...On/Off settings
DEBUG           0               # [NO]DEBUG 0-2
CLONE                           # [NO]CLONE
NOCLEAN                         # [NO]CLEAN
SAVEEMIS                        # [NO]SAVEEMIS
NONEWLOG                        # [NO]NEWLOG
DOTZ                            # [NO]DOTZ
KEEPD2                          # [NO]KEEPD2
NODUPMET                        # [NO]DUPMET
NOKEEPWIFD2                     # [NO]KEEPWIFD2
NOWIFREPRUN                     # [NO]WIFREPRUN
NOEMISSITE                      # [NO]EMISSITE
```

Table 7.2. femisdei Command Line Options

Use: femisdei	<options>...	
-I	<config file>	: configuration file name
-0		: zero pass (just show settings)
-v		: show version of FEMISDEI
-V		: show RCS version of FEMISDEI
-help		: show help messages
-halt		: halt other version of femisdei
-kill		: kill other version of femisdei
-purge		: delete saved files from/to EMIS
-[no]keepd2		: keep vs. delete existing D2PC cases [keep D2]
-[no]keepwifd2		: keep vs. delete exiting "what if" D2PC case
-[no]wifreprun		: allow "what if" cases to replace "run" cases
-[no]dupmet		: duplicate Met in both exercise and real
-[no]dotz		: convert times to GMT [convert to GMT]
-[no]onepass		: one pass (process one file) [multi-pass]
-[no]clone		: clone a background process [do not clone]
-[no]clean		: cleanup temporary files [do not cleanup]
-[no]saveemis		: save EMIS files [do not save]
-[no]emissite		: use EMIS site codes [do not]
-[no]newlog		: create new log [append to log]
-[no]log	<log file>	: name of log file [no log file (screen)]
-[no]debug	<level>	: debug level (0,1,2) [no debug]
-sleep	<seconds>	: number of seconds to sleep
-daiint	<num sleep iter>	: num sleep iterations between DAI checks
-exercise	<number>	: exercise number
-ep	<emis path>	: directory for incoming EMIS files
-pf	<profile file>	: profile file name
-fev	<host> <port>	: fev host port
-ftp	<host> <user> <path>	: ftp host username path
-dei	<dei path>	: top-level directory for DEI output files
-ora	<user/pass>	: Oracle username and password

8.0 FEMIS Data Acknowledgment Interface (DAI)

The Data Acknowledgment Interface (DAI) sends data receipt acknowledgments from the offpost EOCs back to the onpost EOC from which the data originated. It does this for all event notifications, D2PC cases, work plans, and Protective Action Recommendations (PARs) that are sent from onpost to offpost by writing an acknowledgment in the shared journal when the data actually arrives at each offpost EOC. Therefore, you can verify a particular piece of data arrived at a particular EOC by looking at the shared journal within FEMIS.

If EMIS is part of your site configuration, then these data acknowledgments are also forwarded to EMIS.

8.1 Software and Hardware Components

The FEMIS DAI consists of the software and hardware components listed in the following sections.

8.1.1 Software Components

The FEMIS DAI consists of three software components:

1. The following are Oracle stored procedures in the onpost FEMIS database that alert DAI when the data has been sent:

   p_insert_data_ack_d2
   p_insert_data_ack_wp
   p_insert_data_ack_event
   p_insert_data_ack_par
   p_insert_data_ack_rows

2. The Oracle job (pkg_data_ack_queue.p_acknowledge) that is running in the onpost FEMIS database acknowledges when the data actually arrives at each offpost EOC.

3. The FEMIS/EMIS Data Exchange Interface program (femisdei) forwards data acknowledgments to EMIS. This component is only needed if EMIS is part of your site configuration.

8.1.2 Hardware Components

FEMIS onpost UNIX computer
EMIS UNIX and PC computers (optional)

8.2 DAI Program Detail

Per the software components list, DAI is made up of several interrelated pieces or processes. If all the processes are setup correctly at installation time, there should be no system administration required for DAI. However, the DAI processes will be described here to allow a better understanding of the system. If you are having trouble with DAI, please see Section 8.3, DAI Troubleshooting.

The first step in DAI is to alert the database when there is data being sent from onpost to offpost, which will require an acknowledgment. This is done automatically within the FEMIS and DEI software by calling one of the p_insert_data_ack_xxxx stored procedures at the time the data is being sent offpost. Each of these stored procedures writes records in the data_ack table of the onpost database. This data_ack table acts as a processing queue, and unless data has been sent offpost recently, this table should contain zero records. At the time data is sent offpost, there will be one record per offpost EOC per item of data inserted into this table. For example, if there are seven offpost EOCs and you just sent off a PAR and D2PC case, there will be seven records written for the PAR and seven more records for the D2PC case written to the data_ack table.

The next step in DAI process is for the Oracle job pkg_data_ack_queue.p_acknowledge to wake up and check if there are any records in the data_ack table which need to be processed. If there are records, this Oracle job will use the information contained in the data_ack table to remotely check the offpost snapshots for the data in question. If it finds that the data has indeed made it to the specific offpost snapshot, a shared journal entry will be added which states this on an EOC-by-EOC basis. If the data has not made it to a particular EOC, a counter will be incremented for that data_ack record, and it will be checked again the next time the Oracle job runs. If the Oracle job runs six times, and still fails to find that the data has been replicated offpost, then a shared journal entry will be added saying the data did not make it to the specific EOC. The Oracle job runs once every two minutes.

The final step in the DAI process only occurs if the site includes EMIS in its configuration. At regular intervals, the DEI will check if there are any data_ack entries that have been tagged as either arriving or not arriving offpost. If it finds any such entries, they are forwarded to EMIS in the key.dat file, and deleted from the data_ack table. If there is no DEI in the site configuration, then the data_ack records will have already been deleted by the pkg_data_ack_queueu.p_acknowledge job. The Oracle job knows whether there is a DEI in the site configuration based on the dei_used flag in the EOC table. This flag should be set at installation to either y or n. The interval at which the DEI checks records in the data_ack table is controlled by the daiint parameter within DEI. The default is to check every 60 seconds. For more information about this parameter, see Section 7.0, FEMIS Data Exchange Interface (DEI).

8.3 DAI Troubleshooting

The most thorough way to test if DAI is working is to send something, such as a D2PC case, offpost from within EMIS or FEMIS, and then check the shared journal after a few minutes to make sure that the data was acknowledged at all of the offpost EOCs. This process is the recommended check for new installations.

Another way to check is to determine if the AutoRecovery process is reporting any DAI errors. Assuming DAI was configured correctly at installation, this would be all that you need to check. This same information may be gathered by using FWATCH on the PC.

Below are some troubleshooting checks you might make at installation and some others for day-to-day operations.

8.3.1 Troubleshooting at Installation

The database needs to include all of the following packages/procedures:

```
p_insert_data_ack_d2
p_insert_data_ack_wp
p_insert_data_ack_event
p_insert_data_ack_par
p_insert_data_ack_rows
pkg_data_ack_queue
```

If you are not sure if these are really loaded, you may get into SQLPlus for the onpost EOC and issue the following query:

```
select distinct name from all_source;
```

All the names listed above should be included. If they are not, you will need to run the scripts to create them. These scripts should be found in the onpost server's /home/femis/database/proc directory. If you need to insert pkg_data_ack_queue, you will also need to insert pkgb_data_ack_queue. Please contact PNNL should any of these procedures/packages be missing from the database at installation.

The database needs to include database links from the onpost database to all the remote offpost databases. This is generated by running the cr_dai_script.sql, which is run automatically at installation time.

Verify that the EOC table has the correct value for dei_used. You may do this from SQLPlus on the UNIX server for the onpost database with the following query:

```
select dei_used from eoc;
```

If you are getting onpost information from EMIS, this flag should be set to y. If you are not getting onpost information from EMIS, this flag should be set to n. If you need to change the value, **issue only one** of the following commands from the onpost database through SQLPlus:

```
update eoc set dei_used='y';
```

or

```
update eoc set dei_used='n';
```

8.3.2 Day-to-Day Troubleshooting

DAI needs minimal day-to-day troubleshooting. If the Oracle job (pkg_data_ack_queue.p_acknowledge) stops, FEMIS AutoRecovery automatically restarts it. If you wanted to restart it yourself, you could do so by running the startdai.sh script while logged into the onpost UNIX machine as femis. It will not hurt anything if you run this script more than once, since the script will first kill any old instances of the Oracle job before starting a new one. There is also a stopdai.sh script which stops the DAI Oracle job, but if you wish to use this for some reason, remember that AutoRecovery will restart DAI for you the next time AutoRecovery runs. If you wish to turn off DAI and leave it off, you will need to configure AutoRecovery not to restart DAI.

9.0 FEMIS GIS Database

The FEMIS spatial data resides on the UNIX server and on each PC that is running FEMIS. The master copy of the spatial database resides on the server and contains the static GIS themes, the FEMIS ArcView GIS project file (FEMISGIS.APR), the GIS initialization file (FEMISGIS.INI), two map symbol files (MARKERDF.AVP and OBJ_TYPE.LUT), several bitmap (.BMP) files that provide images for special-purpose buttons on the custom ArcView GIS interface, and initial versions of the dynamic GIS themes. When FEMIS is first installed on each PC, the spatial database files for the relevant CSEPP hazard site are copied from the server to the \FEMIS\GIS\<SITE CODE> directory and associated subdirectories on the PC. During subsequent FEMIS version upgrades, selected spatial data files may be copied to a PC as necessary to apply changes or additions to the spatial data.

The following paragraphs discuss the components of the spatial database and the methods used to maintain, configure, customize, backup, and troubleshoot the spatial database.

9.1 Spatial Data Description

The FEMIS spatial database is made up of a number of themes or layers. Each theme contains data (location information and descriptive attributes) representing a collection of geographic objects of a particular type (e.g., roads, political boundaries, meteorological towers, emergency planning zones). The spatial database also contains a customized ArcView GIS project file, an initialization file that tells ArcView GIS what themes are to be loaded into the project file and how to display them, and an optional legend file associated with each theme that provides additional information on how to display the theme's data on the map. For detailed descriptions of the individual FEMIS spatial data themes, please refer to Section 3.3, Building Spatial Data, in the ***FEMIS Data Management Guide***.

9.2 Spatial Data Maintenance

The static spatial data themes are built from various data sources. These themes normally change infrequently, and such changes are made either by regenerating the entire theme from new or updated data sources or by making minor editing changes in the existing theme data. For detailed information on how to maintain or upgrade the static data themes, please refer to Section 5.0, Managing Spatial Data, in the ***FEMIS Data Management Guide***.

As FEMIS is being run, the data in the relational database that corresponds to the dynamic spatial data themes (e.g., facilities) may be altered by users that have the appropriate FEMIS privileges. As necessary during its operation, FEMIS automatically regenerates the spatial data files for these dynamic themes on each PC based on the current data in the relational database. No additional action by the system or data administrator is necessary to maintain these themes under normal circumstances.

9.3 CSEPP Zone Editor

The CSEPP Zone Editor allows sites to make modifications to the GIS Emergency Planning Zone Theme. Changes are made in the GIS Zone theme, then the Oracle database information is updated. The final step is distribution of the new GIS Zone theme. Changes to the zones could make existing Risk Areas invalid. You may want to delete existing Risk Areas before using the Zone Editor. The zone editor can only be applied to CSEPP zones. If changes are required for other hazard "zone" themes, contact PNNL for assistance.

Each step is described in the following sections. Prior to beginning zone editing, please contact PNNL for an updated script to be used in Section 9.3.2, Updating the FEMIS Database.

9.3.1 GIS Operations

Zone editing in the GIS uses four zone menu options under the ArcView GIS Edit menu. This capability is only available if the user has GIS Full Access privileges. In the beginning, only the Start Zone Editing option is visible in the Edit menu. The other three options are enabled only if a NewZones.shp theme is added to the view.

Step 1: Start Zone Editing

Ensure you have GIS Full Access privileges. Log in to FEMIS and start the GIS from the FEMIS Map button on the toolbar. If you have full access privileges, the F button will be enabled. Press the F button on the ArcView GIS toolbar to change to the full GIS capability. Under the Edit menu option, select the Start Zone Editing option. The theme NewZones.shp is added to the current view. If NewZones.shp does not exist in the zone directory, FEMIS will create it by copying the existing zone theme to the file NewZones.shp.

Step 2: Edit the NewZones.shp Theme

When the NewZones.shp is loaded, edit it using standard ArcView GIS editing functionality. Name and zone ID can also be modified in Step 3 using the Change Zone Attributes menu option.

Step 3: Execute the Change Zone Attributes Option

Before allowing any changes, this option checks the NewZones theme structure to make sure it complies with the rules below. You can review this structure in the GIS by activating the zone theme in the GIS and clicking the Table button. After edits have been made, the zone editor will provide warning messages if your structure is not consistent with the rules below. Avoid changing the existing order of the fields.

- All FEMIS required fields are of type CHAR except for zone_id, which is numeric.
- The shape field should contain the value polygon.
- The zone_id field should be numbers of less than 10 digits.
- The Type field should be 8 or less characters.

- The Zone field should be 30 or less characters.
- The Par_Pad field should be 20 or less characters.
- The Risk_Area field should be20 or less characters.
- The Objecttype filed should be identical to the Type field in both structure and entries.
- The Objectname field should be identical to Zone field in both structure and entries.
- Each zone must have a unique ID and name.
- Additional fields are also permissible and should be added at the end of the existing list of fields.

This Change Zone Attributes option lets the user modify the zone name and type for all selected zones. You may run the script several times, if needed. The name and ID changes are immediate. If you make an error, you can repeat the operation with the correct information. If necessary, you can delete the NewZones.shp file and begin again.

Step 4: Create Text Files Listing Zone Attribute Changes

Under the ArcView GIS Edit menu, select the Promote Zone Attribute Changes to DB option. This option creates the input files needed to promote the changes to the database as described in Section 9.3.2, Updating the FEMIS Database. The two files created are ZONENAMECHANGES.TXT and ZONETYPECHANGES.TXT. These files will be written in the GIS home directory (specified as the GISTopDirPC in the FEMIS.INI file). The option creates the files by comparing the old and new zone shape files and writing the changes to the aforementioned two files.

Before performing any comparisons, this option checks whether the zone IDs and names are unique. If not, the user will be notified and no comparisons will be performed. The user will need to return to Steps 2 or 3 to make zone names and IDs unique.

The format of the ZONETYPECHANGES.TXT is as follows:

|ID|old_type|new_type|

There will be one record in the ZONETYPECHANGES.TXT file for each renamed or added zone.

- **Renamed zones** will have all fields. The old_type may be the same as the new type if there was only

- **New zones** have a null old_type and the appropriate zone type in the new_type field.

The format of the ZONENAMECHANGES.TXT is as follows:

|ID|old_name|new_name|zone_type|zone_num|eoc_name|

There will be one record in the ZONENAMECHANGES.TXT file for each deleted, renamed, or added zone. Except as noted below, none of the fields should contain null values.

- **Deleted zones** will appear as the first records in the ZONENAMECHANGES.TXT file. For deleted zones, the new_name is null. The deleted IDs will not be listed in the Type file.

- Records for **renamed zones** will follow the deleted zone information in the text file. For name changes, the record lists the zone ID, the old zone name, new zone name, and zone type.

- **New zones** will list the zone number, have a null old_name, and the EOC with primary responsibility for the zone.

The number of changed records is reported in an interactive message to the user. If an error occurs, use the ERRORLOG.TXT file in the GIS home directory to troubleshoot the problem.

Step 5: Create Text File Listing Facility-Zone Relationship Changes

Under the Edit menu option in ArcView GIS, select the Promote Point-In-Zone Changes to DB option. This option creates the file FACWITHZONECHANGES.TXT. FACWITHZONECHANGES.TXT is the input file needed to make changes to the zone-facility relationship in the Oracle database. The file will be written in the GIS home directory (specified as the GISTopDirPC in the FEMIS.INI file).

The format of the FACWITHZONECHANGES.TXT file is as follows:

|facility_name|eoc_name|old_name|new_name|

The file contains a record for every facility that has been affected by the zone changes.

- If a facility used to be inside a zone's boundary, but now falls outside any zone boundaries, the new_name will be set to null.

- If a facility used to be outside zone boundaries but is now within a zone, the old_name will be null.

- If a zone change changes the zone in which a facility is located, all fields will contain data.

Before performing any comparisons, this process will check whether the zone IDs and names are unique. If not, the user will be notified and no comparisons will be performed. The user will need to return to Step 3 to make zone names and IDs unique.

The number of changed records and the list of changes are also reported to the user in an interactive message.

Step 6: Examine the Text Files and Make Corrections, If Necessary

It is essential that the .TXT files are correct to avoid corrupting the Oracle database. Review the files using a text editor to make sure the following conditions are met.

Ensure that each file ends with a carriage return.

Null values are not allowed in the first field (ID) in any of these files. The other parameters must be compatible with the format of the fields in the database. For example, for zone name changes, the old_name and new_name must be 30 characters or less and must begin with alpha character.

For the ZONETYPECHANGES.TXT file, nulls are only allowed for the following conditions. All other nulls should be replace with the appropriate information.

- old_type is null for new zones.

For the ZONENAMECHANGES.TXT file, nulls are only allowed for the following conditions. All other nulls should be replaced with the appropriate information.

- old_name is null for new zone records.
- new_name is null for deleted zones.
- zone_type may be null for deleted zones.
- zone_num may be null for renamed zones and deleted zones.
- eoc_name may be null for renamed or deleted zones. Ensure it is the eoc_name rather than the eoc_code.

For the FACWITHZONECHANGES.TXT file, ensure there are no null fields and that the eoc_name field contains the eoc_name rather than the eoc_code. (In certain cases, the GIS can not determine the eoc_name, so inserts the eoc_code instead.) Use the editor to replace the eoc_code with the eoc_name.

9.3.2 Update the FEMIS Database

When the GIS editing has been completed, follow the steps below to update the FEMIS database. The steps assume the user is familiar with text editing and updating the Oracle database using SQL scripts.

1. Ensure the /home/femis/database/zonedt directory exists. If this directory does not exist, create it. If zone editing has been done before the directory will exist; you may want to rename or move the existing *.txt and *.sql files to preserve the previous edit files.

2. Move the three output files created in Section 9.3.1 from the PC to the UNIX server into the /home/femis/database/zonedt directory. Copy the zone_edit_db.sh file from the /home/femis/database/dba directory to the /home/femis/database/zonedt directory.

3. Execute the UNIX shell script named zone_edit_db.sh. If this is the first time you have done zone editing, contact PNNL for an updated zone_edit_db.sh file. The script will check on environment variables and for the presence of the eoclist.dat and eocnum.dat files in the /home/femis/etc directory. If all conditions are OK, the script will read the three .txt input files and produce one output file, which contains the actual scripts to modify the database. The output file is named zone_type_change.sql. Review the zone_type_change.sql file to ensure all changes have been included.

4. Reset the Oracle database passwords to the default values. (See Section 13.2.3, Password Change Tool, for instructions.)

5. Commit the database changes by running the output script using the SQLPlus tool. If any errors are noted, stop the process using Ctrl+C, and fix the problems.

6. Reset the Oracle database passwords to their more secure values. (See Section 13.2.3, Password Change Tool, for instruction.)

9.3.3 Distribute the New Zone File

To complete the zone editing process, rename NewZones.shp shape files to the old zone theme name (e.g., <sitecode>_ez.shp). (These files are both located in the <GIS DRIVE>\FEMIS\GIS\<SITE>\ZONE directory on the PC used to do the GIS editing). Copy it to the GIS directory of all the PCs in all EOCs replacing the old theme. The FUPDATE utility described in Section 4.6, Guidelines for Updating All PCs at an EOC with New Files, in the ***FEMIS Installation Guide*** may be used. Also replace the zone shapefile on the master copy of the spatial database which resides on the server so future installs will use the updated zone file.

9.4 GIS Configuration

When you install FEMIS using the full GIS installation option, the complete GIS directory structure and all data files referenced by the selected FEMISGIS.INI file (see the following paragraph) are copied from the server to the FEMIS\GIS\<SITE CODE> directory and associated subdirectories on your PC. This may take several minutes, depending on the volume of data to be copied for your site and the speed of the network.

You will be given an option to choose from among several versions of the FEMISGIS.INI file. The FEMISGIS.INI file specifies primarily the spatial themes that are to be installed and used to build the operational ArcView GIS APR file for use with FEMIS. For most CSEPP sites, three choices will be available: small, medium, and large.

A small or minimum FEMISGIS.INI file installs only the theme files that are essential for running FEMIS (e.g., zone boundaries, igloos, facilities) or provide a minimum map background for location reference (e.g., state and county boundaries, major roads, populated place names). The mid-size FEMISGIS.INI file includes most of the themes, but does not include large image files and other large nonessential themes (e.g., contour lines, streams). A large or maximum FEMISGIS.INI file installs all of the currently available GIS themes for the site.

To have the most complete GIS, choose the largest FEMISGIS.INI option that will comfortably fit within the available memory space on your hard drive. However, additional themes may negatively impact the speed of GIS response. The setup program will provide information on the space required to install each option and the amount of space available on your hard drive. To create a custom GIS configuration that is different from any of the three optional predefined configurations (FEMISGIS.INI files), you will need to copy the largest FEMISGIS.INI file to your PC and then edit it according to the instructions in Section 9.5, Customizing the FEMIS Map.

Upon completion of the GIS data installation, the \FEMIS\GIS subdirectory will contain the FEMPTY.APR and one or more <SITE CODE> subdirectories. Each \FEMIS\GIS\<SITE CODE> directory will contain a number of subdirectories, each subdirectory containing the data files for one or more specific themes. The main \FEMIS\GIS\<SITE CODE> directory will also contain the FEMISGIS.APR and FEMISGIS.INI files. A special subdirectory, \FEMIS\GIS\<SITE CODE>\LOOKUP, contains several bitmap (.BMP) files that provide images for special-purpose buttons on the custom ArcView GIS interface, and two symbol files (MARKERDF.AVP and OBJ_TYPE.LUT) that include information used to generate the theme classification legends. These legends are used to display different map symbols or icons based on the value of a designated attribute within a GIS theme. For example, facilities can be symbolized based on the facility type, such as schools or hospitals. The following section discusses methods you can use to modify symbols in the default symbol lookup table, add new symbols to this table, and change the assignment of symbols to classes of attributes (e.g., facility types) in the FEMIS spatial themes.

9.4.1 Symbol Lookup Table

The symbol lookup table is located in the <GIS INSTALL DRIVE>\FEMIS\GIS\<SITE CODE>\LOOKUP directory under the file name OBJ_TYPE.LUT. The lookup table specifies the symbols to be used to create the theme legends.

Each line consists of seven entries separated by vertical bars as delimiters. Lines that begin with a single quote are comment lines and will be ignored by FEMIS. Blank lines are also ignored.

The first five fields are numbers corresponding to a symbol type, color, size, background color, and outline color. These numbers reference symbol attributes from within the active symbol palettes in ArcView GIS. The fourth and fifth fields are only used in polygonal themes. The sixth entry specifies the theme type or object category, and the last entry specifies the theme subtype or classification label. The symbol type and color numbers designate the order in which the symbols are listed in the FEMIS GIS pallet window using 0 for the first element. The symbol size is measured in "points" (1/72 of an inch). In

An example of the lookup table is listed below. From the facility entries, we can see that school facilities are symbolized with the 89th symbol, colored with the 46th color, and measure 12/72 of an inch.

To customize the lookup table, use the GIS Configuration Editor (see Section 9.5.3) or edit the file.

'Symbol 'number	Foreground color	Symbol size	Background Color	Outline Color	Object Category	Classification Label
6	16	2	0	14	zone	Depot
7	16	2	0	14	zone	IRZ
9	16	2	0	14	zone	PAZ
8	1	2	0	4	county	OR
8	1	2	0	44	county	WA
0	8	2			road	Primary
0	8	1			road	Secondary
1	7	1			road	Local
.						
.						
.						
26	46	10			tcp	Access
26	51	10			tcp	Traffic
26	50	10			tcp	Traffic/Access
26	51	10			tcp	#NULL#
.						
.						
.						
125	51	10			facility	airport
89	46	12			facility	school
96	46	14			facility	shelter
.						
.						
.						

9.4.2 Symbol Defaults

The MARKERDF.AVP file contains the symbols loaded in the default FEMIS symbol palette. You may change these symbols using the generic ArcView GIS palette window functionality. You may use any of the other symbols provided by ArcView GIS in the C:\ESRI\AV_GIS30\ARCVIEW\SYMBOLS directory. You may also import symbols from ARC/INFO or icons in raster format. If you delete or change the sequence of the existing symbols, then some of the FEMIS GIS "look and feel" will change. For example, if you change the 42nd symbol from a cross hair to an asterisk, then the object (e.g., facility) locations in the FEMIS GIS will be depicted with an asterisk instead of the familiar cross hair. You may add new symbols at the end of the palette and use the symbol lookup table (Section 9.4.1, Symbol Lookup Table) to refer to the new symbols.

9.5 Customizing the FEMIS Map

You can customize the content and appearance of the FEMIS map by editing the original FEMISGIS.INI file or any of the alternate INI files to create a custom FEMISGIS.INI file that can then be used to create a custom APR. The GIS Configuration Editor, described in Section 9.5.3, can help you edit the

FEMISGIS.INI file and the lookup table. You can add new themes; delete existing themes; change the minimum or maximum scale display thresholds; modify the type, color, and size of line or point map features; change the legend names; designate the label (and if applicable, classification fields); specify the default classification fields; designate an alternative directory (and if needed, an alternate drive) for the data source of non-point themes; and control which themes are visible by default when the GIS is first started. A detailed description of the fields in the FEMISGIS.INI file is in Section 9.5.1, Customizing the FEMISGIS.INI File. You can also import your own symbols from other ArcView GIS, ARC/INFO, or raster icons by changing the symbol lookup table and the FEMIS default palette as described in Section 9.4.1, Symbol Lookup Table.

If you customize your FEMIS Map, please keep track of the changes to ensure they can be retained during future FEMIS or GIS upgrades.

9.5.1 Customizing the FEMISGIS.INI File

The FEMISGIS.INI file contains data required to initialize GIS parameters that generate the FEMISGIS.APR and to ensure proper GIS contents each time the FEMIS GIS is invoked by the FEMIS application. An example of the FEMISGIS.INI file is shown at the end of this section. The contents of the FEMISGIS.INI file are discussed below.

The FEMISGIS.INI files is automatically updated anytime you define a new dynamic theme or modify an existing one. If you have an abnormal termination of the FEMIS or the GIS, the dynamic themes section of the FEMISGIS.INI file may be corrupted. To restore the file, you can delete all of the theme entries below the facilities theme. These entries are for the User Defined Themes, and they will be regenerated the next time you start FEMIS.

Blank lines are ignored in the FEMISGIS.INI. Lines with a single quote in the first column are recognized as comment lines and are ignored. Vertical bars delimit the data fields in the FEMISGIS.INI. No data value should contain a vertical bar. String values do not need to be quoted.

The [FEMIS_VERSION] section specifies the FEMIS version for which this .INI file can be used. The next line specifies the size of the themes in the current .INI file. Valid size values are small, medium, or large.

The [SITE_CODE] section specifies the CSEPP site code that the GIS data describes. This parameter should be identical to the corresponding site code in the FEMIS.INI file, otherwise the GIS will not work.

The [DEFAULT_HAZARD_THEME] specified the theme that is to be used for the "zone" theme for the current hazard. "Zone themes within FEMIS are used to create risk areas and protective action decisions. Each hazard has a "zone" theme specified for use with that hazard.

The PROJECTION_PARAMETERS] section specifies the UTM (Universal Transverse Mercator) projection and coordinate system parameters required for the site. The parameters shown in the example are for UTM Zone 16 (appropriate for Alabama).

The [AREA_OF_INTEREST] section specifies a geographic area of interest. The area of interest for FEMIS has been set as a rectangle that starts at the origin (lower left corner) of -126.00 degrees longitude and 23.00 degrees latitude and spans 58 degrees longitude (first size parameter) and 27 degrees latitude (second size parameter). This covers the continental United States. The area of interest is specified to minimize the consequences of ill-defined data points. In certain circumstances, the user is given the opportunity to define the longitude and latitude where an event has occurred. FEMIS GIS does not allow the specification of plumes or threat wedges that originate outside the area of interest.

The theme parameters sections specify the configuration for the themes to be loaded in the FEMIS GIS. The two sections are: [STATIC_THEMES] and [DYNAMIC_THEMES]. The dynamic theme flag is determined based on the section in which the theme is listed. Parameters for each theme are discussed below. The same information is included as comments in the FEMISGIS.INI file itself. It has been omitted from the example to conserve space.

- Theme – Indicates the theme name in the FEMIS Database.

- FEMIS Access – For Feature themes this column contains a "Yes" or "No" to indicate whether the theme is in the FEMIS object table. For Image themes, this column contains "None" or the name of an image catalog to be created. If the name of an image catalog is listed, the image catalog should be described in one of the theme parameter entries of this ini file.

- Type – The theme feature Type column must contain one of the following valid types: Image, ImgCat, point, line, or polygon.

- LoadFlag – This column indicates whether to load the theme ("Yes") or not to load the theme ("No").

- Status – Indicates the visibility of the theme when forming the Apr.

- DisplayOrder – Indicates the order in which themes will appear in the GIS Table of Contents. The theme indicated by the smallest number will appear at the top of the table of contents and will be loaded last (on top of all the other themes). The display order may be negative.

- Label Field – Indicates the field name to be used as the default labeling field.

- Object Category – Indicates the FEMIS theme category. The value must be one of the types listed in the \HOME\LOOKUP\OBJ_TYPE.LUT file. Currently, valid values are zone, county, igloo, facility, tcp, road, and siren. If the value is "None" then the classification field should also be set to none and the default legend field should be set to "simple", indicating the theme may not be classified using the look-up tables.

- Default legend – Indicates whether a simple or classified legend is used. Valid values are "simple", "none", and "classify". "Simple" indicate a simple legend that uses one symbol to depict all the theme data. None is used for image themes for which a classified legend does not apply.

- Default legend – Indicates whether a simple or classified legend is used. Valid values are "simple", "none", and "classify". "Simple" indicate a simple legend that uses one symbol to depict all the theme data. None is used for image themes for which a classified legend does not apply.

- Classification Field – Indicates the field to be used to classify the legend. If the classified legend does not exist it will be created.

- Min Scale – Indicate the minimum scale denominator at which a theme will be displayed.

- Max Scale – Indicates the maximum scale denominator at which a theme will be displayed.

- Legend Name – Indicated the name to be used in the legend in the View table of contents.

- Customize – For Dynamic themes, "Yes" indicates the current symbolization parameters listed in later columns of this record should be used and should not be overwritten when this dynamic theme is updated. "No" indicates the symbol parameters in this record should be overwritten with values from the FEMIS Oracle database when this dynamic theme is updated. Customization is not applicable for static themes so the field should contain "N/A" for static themes.

- Symbol – Indicates the symbol to be used in a simple classification.

- Color – Indicates the foreground color for theme symbols, if they can be colored.

- Size – Indicates the symbol size.

- BackGround Color – Indicates the BackGround Color for polygonal symbols.

- Outline Color – Indicates the outline color of polygonal symbols.

- Path – Indicates the location of the file for the theme. The path is appended to the GIS home directory specified in the FEMIS.INI file for the GIS data under the keyword FemisgisTopDirPC.

- Alternate prefix – Indicates a location other than the one specified in the FEMIS.INI file should be appended to the "path". The script that loads themes appends the "path" to this prefix to locate and read an alternate source directory. This can be used to access data located somewhere other than your PC hard drive. Any auxiliary files will be written using the home prefix.

[FEMIS_VERSION]
FEMIS Version=1.4.6
FEMISGIS Size designation=large

[SITE_CODE]
SiteCode=UMCD

[DEFAULT_HAZARD_THEME]
Theme Name: zone

[PROJECTION_PARAMETERS]
Central Meridian: -117
Reference Latitude:0
False Easting: 499990
False Northing: 7
Scale: 0.99960
Spheroid: SPHEROID_CLARKE1866

[AREA_OF_INTEREST]
origin: -126.00| 23.00
size: 58.00| 27.00

[STATIC_THEMES]

'Theme	FEMIS Access	Type	Load Flag	Status	Display Order	Label Field	Object Cate-gory	Defult Legend	Classifi-cation Field	Min Scale	Max Scale	Legend Name	Customize	Symbol	Color	Size	Back Color	Outline Color	Path	Alter-nate Prefix
lm_1m	None	Image	Yes	off	62	None	None	None	None	750000	2500000	Map Image 1:1M	N/A	1	2	3	0	5	lm_1m\umcdmill.tif	E:\
lm_500k	None	Image	Yes	off	61	None	None	None	None	100000	750000	Map Image 1:500K	N/A	1	2	3	0	5	lm_500k\umcd500k.tif	E:\
ictl24k	None	ImgCat	Yes	on	54	None	None	None	None	7500	50000	Major Cities 1:24K	N/A	1	2	3	0	5	lm_24k\cities24.dbf	E:\
lm_24kWW	ictl24k	Image	Yes	on	53	None	None	None	None	7500	50000	Walla Walla WA 1:24K	N/A	1	2	3	0	5	lm_24k\wlawla24.tif	E:\
lm_24kRi	ictl24k	Image	Yes	on	52	None	None	None	None	7500	50000	Richland WA 1:24K	N/A	1	2	3	0	5	lm_24k\rchlnd24.tif	E:\
lm_24kPr	ictl24k	Image	Yes	on	51	None	None	None	None	7500	50000	Prosser WA 1:24K	N/A	1	2	3	0	5	lm_24k\prossr24.tif	E:\
contour	no	Line	Yes	off	46	Elevation	None	simple	None	100000	500000	Elevation Contours (m)	N/A	0	52	1	0	5	contour\umcdc300	none
cedblock	yes	Polygon	Yes	off	45	Block	None	simple	None	2000	150000	Census Blocks	N/A	0	5	1	0	5	cedblock\umcd_tb	none
Tax_lots	no	Polygon	Yes	off	37	Name	None	simple	None	50	1000000	Morrow Co Tax Lots	N/A	0	19	1	0	5	tax_lots\cmor_tax	none
adminbnd	no	Polygon	Yes	off	35	Name	None	classify	Type	20000	15000000	Administrative Boundaries	N/A	0	55	1	0	5	adminbnd\umcd_ab	none
zone	yes	Polygon	Yes	on	34	Zone	Zone	classify	Type	5000	15000000	Emergency Zones	N/A	0	4 2	2	0	5	zone\umcd_ez	none
state_bd	no	Polygon	Yes	on	33	State	None	simple	None	5000000	0	State Boundaries	N/A	0	5	2	0	5	stcounty\umcd_sb	none
county	yes	Polygon	Yes	on	32	Objectname	County	simple	Objecttype	20000	10000000	County Boundaries	N/A	0	5	2	0	5	stcounty\umcd_cb	none
Railroad	no	Line	Yes	off	30	Name	None	simple	None	500	2|0000000	Railroads	N/A	0	34	1	0	5	railroad\umcd_rr	none
Road_uma	no	Line	Yes	off	29	Fname	None	simple	None	500	1500000	Umatilla Co Roads	N/A	0	8	1	0	5	roadall\cuma_ra	none
Road_mor	no	Line	Yes	off	28	Fname	None	simple	None	500	1500000	Morrow Co Roads	N/A	0	8	1	0	5	roadall\cmor_ra	none
Igloo_p	yes	Point	Yes	on	21	Igloo_Name	Igloo	classify	Content	10	2000000	Igloos	N/A	5	8	12	0	5	igloo_p\umcd_ip	none
zone_dep	no	Polygon	Yes	on	20	Objectname	None	Simple	None	1000	15000000	Chem. Limited Area	N/A	0	10	2	0	5	zone\umcd_dep	none
mettower	yes	Point	Yes	on	19	Namespeed	None	simple	None	1000	2000000	Met Towers	N/A	75	5	14	0	5	mettower\umcd_mt	none
commsite	yes	Point	Yes	on	18	Objectname	None	simple	None	1000	2000000	Communication Sites	N/A	8	8	6	0	5	commsite\umcd_com	none

[DYNAMIC_THEMES]

'Theme	FEMIS Access	Type	Load Flag	Status	Display Order	Label Field	Object Cate-gory	Default Legend	Classifi-cation Field	Min Scale	Max Scale	Legend Name	Customize	Symbol	Color	Size	Back Color	Outline Color	Path	Alter-nate Prefix
kpoly_cmor	yes	Polygon	yes	off	14	ObjectName	None	simple	None	1000	15000000	CMOR Known Polygons	No	8	44	2	0	53	kpoly\kpoly_cmor	none
kpoly_cuma	yes	Polygon	yes	off	13	ObjectName	None	simple	None	1000	15000000	CUMA Known Polygons	No	8	44	2	0	53	kpoly\kpoly_cuma	none
kpoly_sore	yes	Polygon	yes	off	12	ObjectName	None	simple	None	1000	15000000	SORE Known Polygons	No	8	44	2	0	53	kpoly\kpoly_sore	none
kpoly_swas	yes	Polygon	yes	off	11	ObjectName	None	simple	None	1000	15000000	SWAS Known Polygons	No	8	44	2	0	53	kpoly\kpoly_swas	none
FLOOD_cmor	yes	Polygon	yes	off	8	Objectname	None	simple	None	1000	2000000	CMOR Flooded Areas	No	36	28	2	0	34	kpoly\FLOOD_cmor	none
FLOOD_cuma	yes	Polygon	yes	off	7	Objectname	None	simple	None	1000	2000000	CUMA Flooded Areas	No	36	28	2	0	34	kpoly\FLOOD_cuma	none
FLOOD_sore	yes	Polygon	yes	off	6	Objectname	None	simple	None	1000	2000000	SORE Flooded Areas	No	36	28	2	0	34	kpoly\FLOOD_sore	none
FLOOD_swas	yes	Polygon	yes	off	5	Objectname	None	simple	None	1000	2000000	SWAS Flooded Areas	No	36	28	2	0	34	kpoly\FLOOD_swas	none
siren	yes	Point	Yes	off	4	Objectname	None	simple	Objecttype	1000	2000000	Sirens	Yes	26	32	12	0	5	siren\siren	none
known_p	yes	Point	Yes	off	3	Status5	None	simple	Objecttype	1000	2000000	Known Points	Yes	16	44	12	0	5	known_p\known_p	none
tcp	yes	Point	Yes	off	2	Objectname	tcp	simple	Objecttype	1000	2000000	Traffic Control Points	Yes	51	29	24	0	5	tcp\tcp	none
facility	yes	Point	Yes	on	1	Objectname	facility	classify	Objecttype	1000	0	Facilities	Yes	1	50	6	0	5	facility\facility	none

9.5.2 Altering the Default FEMIS Map

To alter the default appearance of the FEMIS map, use the Use at Startup option for FEMIS GIS ViewMarks (See the Online Help). For more extensive changes, complete the following steps:

Step 1 Copy or rename the original \FEMIS\GIS\<SITE CODE>\FEMISGIS.INI file to another name (e.g., FGISORIG.INI) so you can retrieve it and use it later, if necessary. Do the same with the original APR (e.g., copy and rename it to \FEMIS\GIS\<SITE CODE>\FGISORIG.APR). Then make another copy of the original INI file or one of the alternate INI files. Use the GIS Configuration Editor or manually edit the copy to

a) To exclude themes, remove (or comment out using a single quote in the first column) lines defining existing themes that you want to exclude, or specify No in the load flag.

b) Add lines to define new themes.

c) Modify the appropriate parameters of existing themes as desired.

Step 2 Run ArcView GIS using the empty project file, \FEMIS\GIS\FEMPTY.APR, by double clicking on the file name in the Windows File Manager. When the APR has finished loading, it will contain the FEMIS static themes indicated in the FEMISGIS.INI files and will create the FEMISGIS.APR file in the GIS home directory (\FEMIS\<SITE CODE>\GIS). When the FEMIS application loads the FEMISGIS.APR, the changes made to the dynamic themes will be depicted.

Step 3 Examine the theme legends to see that the correct set of themes was loaded and the correct ones are visible. The dynamic themes will not appear in the legend at this time. These themes are loaded when FEMIS use the FEMISGIS.APR. Then examine each theme to see that it displays correctly (check the checkbox in the legend to make visible the themes that are invisible by default). If some themes are not displayed correctly, recheck the INI file. If necessary, exit ArcView GIS, edit the INI file to make corrections, and then repeat Steps 2 and 3.

Step 4 Exit ArcView GIS. Use Windows Explorer to set the FEMISGIS.APR file access properties to Read-only. The FEMISGIS.INI and FEMISGIS.APR files you just created will be used each time the FEMIS GIS is started.

9.5.3 GIS Configuration Editor

The GIS Configuration Editor is a stand-alone program that provides an easy to use interface for modifying the FEMISGIS.INI and OBJ_TYPE.LUT files.

Note: Make a backup copy of the FEMISGIS.INI and OBJ_TYPE.LUT files so that you can recover from an unsatisfactory editing session.

The [SITE_CODE], [DEFAULT_HAZARD_THEME], [PROJECTION_PARAMETERS], and [AREA_OF_INTEREST] sections of the FEMISGIS.INI file can be modified on the main window. The [THEME_PARAMETERS] section is displayed in a spreadsheet on the main window.

To modify an individual spreadsheet entry, select the row and click the Details button or double-click on the row. The GIS will be started and a details window will be displayed for that row. A single quote found at the beginning of a line indicates a comment line and FEMIS ignores the line. All the fields are described in Section 9.5.1, Customizing the FEMISGIS.INI File. The symbol parameters for shape, color, and size can be entered using the text boxes or by clicking the Map button and selecting a symbol from the palette. The GIS can be used to visualize the symbols and determine the appropriate symbol parameters.

If the Map button is pressed, the GIS will be brought in the foreground with the ArcView GIS palette active.

Use the ArcView GIS palette to modify the color, shape or fill pattern, and size of the drawn symbol. When satisfied with the symbol appearance, click the Return Symbol Parameters button. The appropriate numbers for the symbol color, shape or fill pattern, and size will be returned to the details window. The size is measured in 1/72 of an inch. For lines, it designates width. For polygons, the size is used for the width of the outline.

The Legend Symbol tab is used to add, edit, or delete entries from the OBJ_TYPE.LUT file. The symbol parameters for shape, color, and size can be entered by using the text boxes or by clicking the Map button. The GIS can be used to visualize the symbols and determine the appropriate symbol parameters.

If dynamic themes or the OBJ_TYPE.LUT file have been modified and saved, close the GIS and restart to implement the changes. For static themes, once the changes have been saved to the FEMISGIS.INI file, follow the instructions found in Section 9.5.2, Altering the Default FEMIS Map, to alter the default FEMIS map.

9.5.4 Theme Projection Utility

FEMIS uses the projected theme data in Universal Transverse Mercator (UTM) coordinate system in order to avoid reporjecting geographic coordinates each time the view is refreshed. To include new themes into FEMIS they should be converted to UTM. The Theme Projection Utility converts feature themes in geographic coordinates to UTM coordinates for the desired CSEPP site. Image themes, which are required to be in projected coordinates, are skipped by the Theme Projection Utility. Image themes not already in UTM would need to be modified using other software such as ARC/INFO.

When you open PROJECTION_UTILITY.APR, ArcView GIS will start and a window containing two Views will display. View1, the work area, is on the left side; and View2, where the results are depicted, is on the right side.

The Theme Projection Utility assumes that the input themes are in geographic coordinates and will let you select themes from a list of existing shape files in View1 so they can be exported as projected shape files using the currently specified projection in View1. The exported files are added to View2.

To use the this utility complete the following steps:

1. Double-click on the Projection_Utility.Apr (usually located in your C:\FEMIS\GIS directory).

2. Click View → Properties → Projection.

3. Select the Standard radio button, and Geographic will display in the Type field.

4. Load the themes you want to project. Click the + (Add Theme) button.

5. Click the Export Projected item under Utilities, and click OK on the brief information window that displays.

6. Select the desired CSEPP site from the list, and click OK.

7. Make any necessary adjustments to the UTM projection parameters for the selected site, and click OK.

8. Navigate to the desired directory or accept the default (usually C:\TEMP), and click OK.

9. Select the themes you want to export from the list of the themes in View1, and click OK.

   If the name of the theme being converted already exists in the selected directory, a temporary name will be suggested for the converted theme. Click OK to accept the temporary theme name.

   The conversion process will start and the status bar will indicate the progress of conversion. The new theme(s) will be loaded in View2 so you can visually verify the results. You may want to load some of your other themes, like raster images, to check how well the projected coordinate match the existing themes.

10. Click Exit under the File menu to close the PROJECTION_UTILITY.APR file. Click No on the message about saving changes to this file.

9.6 Backup Procedures

The installation directory for the spatial data on the UNIX server is /home/femis/gis. This current operational GIS data is copied to the PCs when FEMIS is installed or upgraded. It is recommended that a tar tape of this directory be made each time a new version of FEMIS is received. The tape should be

labeled "FEMIS GIS Data" with the date and FEMIS version number included. If the GIS data on the server should become corrupted or deleted, the spatial data can be restored from the backup tar tape without having to perform a reinstallation of FEMIS on the server.

If a site customization of the spatial data and/or the APR and INI files is to be done, the original GIS data directory should first be copied to another directory (e.g., /home/femis/data/v<x.y>/gis, where <x.y> is the FEMIS version number associated with the released data. A second tar tape of the GIS directory should be made following the completion of the GIS customization.

9.7 GIS Database Troubleshooting

A number of factors can cause errors in loading or displaying the spatial data themes or undesirable display behavior or appearance. Some of the more common problems are listed below, along with some suggestions for finding and correcting the problems.

1. Zoom to All Themes may cause displayed themes to shrink to a very small portion of the display screen, or to disappear entirely. This is typically caused by themes having one or more objects with "improper" latitude/longitude coordinates, e.g., (0,0) or any point that is far from the "area of interest" surrounding the hazard site. For most of the point themes, you can check the attribute table associated with the theme (activate the theme legend and click the Table button in the ArcView GIS button bar). Search the latitude and longitude columns for values that are noticeably different from the majority of objects in the theme. Attempt to verify the correct coordinates for points that are suspected to be outside the area of interest.

2. Error messages similar to Unable to Access Theme or Index Out of Range may occur when attempting to access the GIS. These errors are most often caused by improperly defined themes, such as an empty theme (a theme with zero map objects). Check the text file (.EVT file) associated with all dynamic point themes to make sure each theme contains at least one data line in addition to the header (column names) line.

3. Classification errors may occur when attempting to load theme data into an empty APR. They can occur on themes with legends that classify and display the map objects based on a column in the theme's attribute table (e.g., zones are classified and displayed by zone type: Depot, PAZ, IRZ.). The error could be caused by the wrong field name being designated as the classification field in the FEMISGIS.INI file. Check the attribute table of the offending theme in the APR.

   The error could also be caused by a new data value for the classification column that was not included in the values defined in the theme's legend (.LEG) file. Regenerate the FEMISGIS.APR from the empty APR using the process described in Section 9.5, Customizing the FEMIS Map. Make sure that all the entries in the classification field are included in the \FEMIS\GIS\<SITE CODE>\LOOKUP\FEMISGIS.LUT file.

4. Display refresh delays may occur during zooming. For example, the GIS may take an inordinate amount of time to refresh the map display when zooming into a very small area of the map. These lengthy delays can usually be attributed to one or more of the larger themes (map images or vector themes with a large amount of data) that does not have an appropriate lower display limit. To check the display limits of a theme, activate the theme legend, then select Properties under the Theme menu, then click Display. The minimum scale should never be less than 10 for themes with a large amount of data, such as roads, streams, census block boundaries, or raster map images. A larger minimum scale (e.g., 100) may help to reduce the zoom-in redisplay time significantly.

5. The appearance of raster map images may be degraded and may detract from the viewing of other themes if displayed at an inappropriate scale factor. Follow the procedure described in Item 4 above to check the display limits of a map image theme and set the limits to appropriate values for the map scale at which the original scanned map was created. If the image is allowed to be viewed at scales that are too small compared to the map's base scale (e.g., 1:200,000 for a 1:24,000 scale quad sheet map), the image will appear too small to be readable and will clutter the display. If the image is allowed to be viewed at scales that are too large (e.g., 1:1,000 for a 1:24,000 scale map), the individual pixels of the digitized map will be enlarged so much as to give the portion of the map being viewed a "blocky" and unfocused appearance. The best scale range will vary depending on the resolution and quality of the scanned image. A general guideline is that the scale value (denominator of the scale ratio, e.g., 24000 for a scale of 1:24,000) should have its minimum set to about 20 percent of the map's base scale value (e.g., around 5000 for the 1:24,000 example), and its maximum set equal to or slightly larger than the base scale value (e.g., around 30000 for the 1:24,000 example). A greater range may be used if the map image is of very high resolution and quality.

6. The FEMISGIS.INI file is automatically updated each time you define a new dynamic theme or modify an existing one. If FEMIS or the FEMIS GIS terminates abnormally, the dynamic themes section of the FEMISGIS.INI file may be corrupted. This can be fixed by deleting all the theme entries in the FEMISGIS.INI below the facilities theme entry and then restarting FEMIS. The entries below facilities in the FEMISGIS.INI are for the user-defined themes and are regenerated from the Oracle database the next time you start FEMIS.

10.0 FEMIS Oracle Database

The relational database in FEMIS is managed by Oracle v7.3.4, a commercial DBMS. The distributed processing features of Oracle are utilized to produce a multi-server distributed data architecture. Data replication is widely used to provide a local copy of most shared tables. This replication is important because it allows an EOC to operate autonomously in case the links to other EOCs are not operational. Also, performance is enhanced because the local tables are located on the local database.

In FEMIS, the FEMIS relational database is made up of approximately 180 tables. The FEMIS logical data model describes graphically what information is present and how the data objects are interrelated. The model represents a large collection of general purpose tables, evacuation data, GIS tables, and dispersion tables. Additional information about the data model is available in the ***FEMIS Data Management Guide***.

Based on design efforts and testing results, each relational database table is local to an EOC or shared with the other EOCs. Data in the local tables can be accessed only by users logged in to that EOC. The data in shared tables is available to several EOCs. Details of data placement are made transparent to the FEMIS users, so the FEMIS database appears to be a single, unified collection of tables. This physical design of the Oracle database is provided as a part of database implementation and should be applicable to all CSEPP sites. More details about the Database Management System (DBMS) are provided in the ***FEMIS Data Management Guide***.

For information on the recommended backup strategy and performing Oracle database backups, see Section 14.0, Backup Strategy for FEMIS.

10.1 Data Description

When creating the first database for a new site or when making major database modifications, it is necessary to create the database structure from scripts and load basic data so the FEMIS application can operate. For most situations, the new database will be created in a development facility and then packaged so it can be delivered to the operational site. Section 3.0, Building the Initial Information, of the ***FEMIS Data Management Guide***, describes how a new database is installed at the site.

For cases where the FEMIS software is updated to a new release, the existing site database can be updated, if necessary, to support new capabilities. In this case, one or more scripts are developed to make the data structure and/or data content modifications. Instead of recreating the database, the scripts are run to make it compatible with the new FEMIS version of software.

10.2 Replication

Oracle provides several ways to share data between EOC servers in a distributed, multiserver environment. When the site environment is not tightly controlled by one group, it makes sense to operate in a mode where operations can proceed in each server independent of what the other servers are doing.

To make this happen, data sharing has to be asynchronous so that data changes in one server are not dependent on making similar changes in the other servers in the same transaction.

In Oracle v7.3.4, data record changes can be propagated to other servers using read — only snapshots. This method is currently used by FEMIS since it is asynchronous and flexible. The server where the change occurs creates a log of the change and waits for remote servers to request updates. If the remote server is up, it periodically sends a request for these updates. In FEMIS versions before 1.2, requests were made on most tables on a 1 minute rate and on the D2PC tables at a 20 second rate. This method of data sharing works well with four or fewer servers but due to constant polling, develops a load on the servers and on the network.

FEMIS uses a method of data sharing for multiple servers. This method is an event driven scheme that still is asynchronous but is less demanding on the servers and network. The design uses change logs but signals the remote servers to refresh their snapshots as the change is made. This reduces the polling overhead at the remote sites and the request traffic on the network.

The current method uses a replicated update table that indicates when a group of snapshots needs to be refreshed due to changes in one or more tables in the group. A local periodic Oracle process monitors the local snapshot of this table to determine when to refresh the snapshots in the groups. Only the new update table is refreshed periodically rather than all of the tables. This allows the number of servers per site to increase to allow each EOC to have a dedicated server.

When the database is installed at a site, either a configuration with all EOCs on a single server or a configuration of several servers is chosen. In the former case there is no replication since the data is shared by Oracle views. If the multiple server option is used, then scripts delivered with the database are run to create the data sharing objects (see Section 2.3.5, Creating or Updating the FEMIS Database, in the ***FEMIS Installation Guide***).

Once the distributed objects are created, replication can be initiated by running the scripts provided. Before doing this, establish that the other servers at the site are in a ready state to be able to participate in data sharing. If a local site is going to be down for several hours or more, replication can be stopped at the other servers by running the stop scripts.

10.2.1 Add Facility Type to FEMIS FACILITY_TYPE Table

The FACILITY_TYPE table is a CSEPP global database table and is not shared between EOCs. If a new facility type is added to an EOC database, it needs to be added to the FEMIS database at all EOCs at the site.

Identify the "type" of new facility you wish to add to the FEMIS database. For this example, we will add a new facility type called Prison.

Enter the FEMIS application by selecting the Database Manager under the Utility menu. The privilege needed to use the Database Manager function is usually only given to the FEMIS System Administrator.

It does not matter what mode you are in since updating the FACILITY_TYPE table is global across operations and exercises. As such, when a new facility type is added, it will be seen by all of the existing FEMIS functionality across operations and exercise.

From the FEMIS Database Manager window, enable the Grid (Read Only) radio button, select the local EOC's FACILITY_TYPE table, and click the Open button. A non-editable snapshot view should be opened that allows you to examine all of the existing facility types. Make sure that the facility type you want to add does not already exist in the FACILITY_TYPE table with a different spelling or a synonym.

Note: Proceed only if you really need to add a new facility type.

Enable the Form (Editable) radio button, then re-select the local EOC's FACILITY_TYPE table, and re-open it. A window containing an editable dynaset for the <eoc>.FACILITY_TYPE will open. Select the Add button and enter the new facility type (e.g., prison). For consistency you should enter the facility type in lower case. Enter the facility type description (e.g., prison) into the empty database administration form. When you are done, select the Update button. The new facility type is added to the EOC's FACILITY_TYPE table. Close the updated form.

Review the contents of the table from a grid. Check to see that the new facility type has been added to the database by accessing Facility under the Data Menu item. Select a facility to enable the Edit button, click on the Edit button, select a facility, and pull down the Facility Type list. The new facility type should be present.

Note: To ensure that the new facility type is also accessible to the GIS, you need to add the new type to the GIS tables as well.

Edit the FEMIS OBJECT_SUBTYPE table to link the new facility type to the GIS.

Start the FEMIS Database Manager by clicking on Start → Programs → FEMIS →Database Manager, and set the Viewing method to Grid (Read `only`), select the local EOC's Object Subtype table, <eoc>.OBJECT_SUBTYPE, and open the table. Be sure there is no record whose LOCATION_TYPE is facility and whose OBJECT_SUBTYPE and FEMIS_OBJECT_DESCRIPTION match the new facility type you just added.

If the new facility type is not in the table, close it and re-open the OBJECT_SUBTYPE table using the editable viewing form.

In the form, select the Add button to enter the new facility type into the table read by the GIS. Make the following entries:

LOCATION_TYPE:	The text facility (must be lower case)
FEMIS_OBJECT_SUBTYPE:	The same facility type you entered in the FACILITY_TYPE table. Be sure they **are exactly the same.**
OBJ_SUBTYPE_DESCRIPTION:	The same facility type description you entered in the FACILITY_TYPE table. Be sure they **are exactly the same.**

Use the Update button to commit the new facility type to the OBJECT_SUBTYPE table. This table is used by the GIS to list the types of facilities that can be located by the GIS.

10.2.2 Testing the Addition of a New Facility Type

After the FACILITY_TYPE and FEMIS_OBJECT_SUBTYPE tables have been updated to contain exactly the same facility type and description, they need to be tested to ensure that they are working properly with the FEMIS application.

To test the new facility type entry in the FACILITY_TYPE table, select Facility under the Data menu. You may want to be in Exercise Mode to ensure that any new facilities you create can be deleted. Select the Add button to create a new facility using the facility type you have just entered into the FEMIS validation tables. In the General tab:

1. Enter the name of the facility.

2. Select the new facility type from the Type pull-down list. If the new subtype appears, the FACILITY_TYPE table was properly updated.

3. Use the Map button to provide the longitude/latitude for the new facility, either by entering values directly or using the GIS to pick a point.

4. Click OK to get the new facility into the database.

To test the new facility type entry from the GIS, enter the Task Status Board, click the Task Details button. When the Task Detail window displays, select the Edit radio button, and click on the Map button on the General tab. The Select Location form appears:

1. Select Facility from the Type pull-down list — all facility types should appear.

2. Select the new facility type you have just added from the SubType pull-down list. You should see the name of the facility you added in the Name list. If the name of the new facility you added appears, everything is proceeding as it should.

3. Use the Map Object button to pick the facility you added to ensure that the GIS also returns the new facility.

If this works properly, the new facility type has been successfully added.

10.2.3 Coordinate the Change to All EOCs

Note: Be sure to have the other EOCs add the new facility to their EOC databases to ensure that the facility information is transferred properly from EOC to EOC. If this is not done, FEMIS will work properly but there will be some inconsistencies in the FEMIS database and user interface screens.

Facilities replicated with the new facility type will be plotted on the GIS map and will appear in the spreadsheet of the facility management interface (select Facility under Data). However, if the receiving EOC does not have the new facility type in its FEMIS database, the type will not appear in the Type menu for the EOC. It will be left blank because that facility type does not exist at that local EOC.

If a user selects another EOC's facility that contains a facility type (from the GIS map via the Select Location interface) which is not in the local EOC's Facility Type table, the facility type returned to the Select Location interface will be (All) instead of the proper facility type. Thus, the changing of facility types should be coordinated with other EOCs and should be performed at the same time.

10.3 Database Maintenance

FEMIS v1.4.6 has a monitoring tool, called AutoRecovery, that continually checks the status of the site's critical hardware and software components. When failures are detected or thresholds are exceeded, warning messages are sent to the system and database administrators. In certain cases, this tool attempts to remedy problems directly. In other cases, the System and Database Administrators must take manual actions to remedy the problems or take measures to correct situations that caused threshold warnings.

AutoRecovery monitors the portions of the database that are most likely to have problems. In most cases, it tries to warn the Database Administrator before the problem causes a serious failure; this is done by thresholds and looking for symptoms of problems, such as network interruptions. In cases where the problem exists and can be resolved, an immediate fix is attempted.

The local database and the database listener are checked each cycle. If the listener is down, a restart is immediately attempted. A database failure is a serious condition that must be analyzed before a restart is attempted since the restart may result in bigger problems. If the database is not functioning, the Database Administrator should look in Oracle's alert log to determine the cause. If the condition is no longer present or has been fixed, the database can be restarted from a command line sequence as follows:

```
> su – oracle        <If not already logged in as the oracle user>
> <pwd>
>svrmgrl
>connect internal
>startup
```

Section 2.0, FEMIS Monitoring Tools, describes the operation of this AutoRecovery tool and other tools that are available to troubleshoot and repair the database. Section 2.6, FEMIS AutoRecovery System Description and Installation, in the ***FEMIS Installation Guide***, discusses how to install these tools and configure them to support the site.

10.4 How AutoRecovery Works with the Database

AutoRecovery monitors the database tablespaces and warns when the thresholds are exceeded. When these warnings are present for an hour or longer, the Database Administrator should take action to prevent the tablespace from reaching the full (or 100% used) condition that will cause a serious database failure. The common causes of tablespace increase are that more data has been added intentionally or some old data, which is not essential, exists in the database. The Database Administrator should check to see if old data is present and if so, remove it. This will cause the tablespace warnings to cease and have the added benefit of increasing system performance by reducing table sizes. The two most common old data types are Met data that has not been archived and extra, nonessential exercises.

If the system has recently added new records to the database intentionally, then the tablespace size should be increased to give a margin for additional growth. The easiest way to do this is to start up the server management Database Administrator tool. To start this tool, enter the following command logged in as the UNIX oracle user:

```
>svrmgrm
```

When the tool comes up, login into the database as the system user. Then choose the storage option to display the tablespace form. Then highlight the tablespace that is overflowing and choose the tablespace menu option, Add Datafile, to bring up dialog to add another file to increase the total tablespace size. Use the online Help for further instructions.

AutoRecovery monitors remote databases and remote listeners and then sends warnings if problems are seen. If these warnings persist, the Database Administrator should notify the remote server administrator of the problem. For some reason, the remote administrator may not be aware (have been notified) that the problem needs to be fixed. In most cases, the problem would be known and one could find out how long the outage may exist.

Database replication is dependent on all components at the network functioning properly including communications, servers, and database. When some failure occurs, replication may not be able to copy database changes. Oracle has built in error recovery that will keep trying up to 16 times, but if all tries are unsuccessful, Oracle will stop and declare that replication is broken. AutoRecovery monitors replication and will attempt to fix errors if there are no current problems on the remote servers. If problems are present, AutoRecovery will continue the warning messages but **will not attempt** to fix the problems—this is why it is important to notify remote system administrators when their systems appear to be malfunctioning.

There are a set of fix scripts that can be used to manually correct replication problems. The Database Administrator should look over these scripts and become familiar with their use. Under normal conditions, AutoRecovery will fix all replication problems.

11.0 FEMIS Evacuation Applications

The FEMIS evacuation interface (fmevac.exe) resides on the PC. The Evacuation SIMulation (ESIM) model resides on the UNIX server and is invoked by the evacuation interface via the FEMIS command server (see Section 4.0, FEMIS Command Server). Import, export, and post processing utilities also reside on the UNIX server to pass information between the ESIM model and the FEMIS database. These utilities, like ESIM, are invoked by the evacuation interface through the FEMIS command server.

11.1 FEMIS Command Server

The command server is used by the evacuation interface via the following three paths:

File-->Import...	(Uses fmevacim utility on the UNIX server)
File-->Export...	(Uses fmevacex utility on the UNIX server)
File-->Run Case	(Uses fmevacex, fmevacrn (ESIM), fmevacpp utilities on the UNIX server).

11.1.1 Import Function

The import function allows the user to import an existing ESIM or IDYNEV evacuation case into the FEMIS database. Once it is in the FEMIS database, it may be run, modified, and/or exported.

11.1.2 Export Function

The export function allows the user to export an existing evacuation case from the FEMIS database to a flat file. This evacuation input file may then be imported elsewhere.

11.1.3 Run Case Function

The run case function extracts input information from the database to create an ESIM input file, runs ESIM, and places the model output into the FEMIS database for reporting/animation.

11.1.4 Operation Status

If the command server is invoked for any of the above operations, a working bar will appear on the evacuation interface. When the operation is complete, the command server notifies the evacuation interface, and the appropriate message is displayed to the user. In addition to waiting for a response from the command server, the evacuation interface polls the command server for a status every 8 seconds. If the process is still running, the working bar is updated. Therefore, if the working bar is updating about every 8 seconds, then the function is still operating.

Note: The working bar does not accurately reflect the percent completion status of the job.

11.2 Directories and Files

Each FEMIS evacuation case has its own directory on the UNIX server. This directory may contain input and output files for the case as well as command server logs for the case. Most of these files may be accessed via the evacuation interface from File → View Output Reports. Below are lists of possible import and export/execute files for each case on the UNIX server:

Import Files:

casefile.mi	Output log for import program
casefile.ini	Control file for import program
nnnnnnn.eri	Log file from command server for import

Export/Execute Files:

nnnnnnn.in	Input file created by export
nnnnnnn.1	ESIM output link statistics
nnnnnnn.2	ESIM output signal information
nnnnnnn.3	ESIM output centroid information
nnnnnnn.4	ESIM output loading information
nnnnnnn.5	ESIM output summary statistics
nnnnnnn.6	ESIM output network-wide vehicle statistics
nnnnnnn.7	ESIM output error report
nnnnnnn.grf	ESIM output link statistics (unused)
nnnnnnn.out	ESIM output cumulative link statistics (unused)
nnnnnnn.inx	Control file for export
nnnnnnn.mx	Log file from export program
nnnnnnn.inr	Control file for model
nnnnnnn.mr	Log file from model
nnnnnnn.inp	Control file for post processor
nnnnnnn.mp	Log file from post processor
nnnnnnn.erx	Log file for command server for export
nnnnnnn.err	Log file for command server for run
nnnnnnn.erp	Log file for command server for post processor
nnnnnnn.ere	Log file for command server for execute.

The directory for a particular case may be found by starting at the directory referenced by FemisUserTopDirNFS in the FEMIS.INI file. From here, the case should be in the subdirectory /evlog/<case id>/e<exercise number>. If you want to find the case ID for your current case, you will find it in the header of any of the output files available under View Output Reports under File, with the exception of the one listed as Error Report. The exercise number is zero for real planning or real operations and user selected for exercises.

11.3 Evacuation and the GIS

Evacuation network information is stored in the database. If users want to view this information on a particular PC, they must click the File → Create Network. The Create Network option uses the most recent graphical information for your current evacuation case to create a network diagram in the GIS. Once Create Network has been selected for a particular case on a particular PC, it does not need to be repeated unless the network is updated on a different PC. When you first open a case, you will be told if you need to run Create Network or if you need to execute the case.

11.4 Show Status

To check the status of your current case, click the Show Status button on the main evacuation window. A message will appear saying whether your local copy of the evacuation network is current and whether the case has been run.

11.5 Oracle Tablespace

Evacuation data require a significant amount of tablespace in the database. It is recommended that you closely manage the evacuation cases in the database. For example, delete cases that you do not want to keep, and do not copy evacuation cases into exercises unless absolutely necessary.

11.6 Troubleshooting for Evacuation Utilities

If for some reason, you cannot import or run an evacuation case through the FEMIS PC interface, you may do so via UNIX scripts as shown below.

> **Note:** Importing or running an evacuation case from the UNIX side should be treated as a last resort for debugging purposes. Running cases through the user interface is the preferred method for importing and running cases.

To import the ESIM model, copy the case to be imported to the EVLOG directory, e.g., /home/femis/user/evlog/1/e0/tead.tdt. Then run a script similar to the following, but substitute your local site values for the values in the example.

```
#!/bin/sh
cmdserv - 9015 <<EOD
run import

DEBUG=Y
IDYNEV=N
CASEID=1
EXERNUM=0
FILENAME=tead.tdt
DATABASE=fi6
```

```
USERNAME=AEMA
PASSWORD=AEMA
WHERE=NW

EOD
```

To execute ESIM model, run the following script.

```
#!/bin/sh
cmdserv - 9015 <<EOD
run execute

DEBUG=Y
IDYNEV=N
CASEID=1
EXERNUM=0
FILENAME=tead.tdt
DATABASE=fi6
USERNAME=AEMA
PASSWORD=AEMA
SUBCODE=ere

EOD
```

12.0 Server Network Time Protocol (NTP) Set Up

The Network Time Protocol (NTP) executables are included with the Solaris v2.6 operating system. Scripts in the FEMIS application configure NTP for the UNIX server and Window NT v4.0. Once NTP has been installed and checked out, all PCs on an EOC's LAN acquire time synchronization from the NTP service running on the UNIX server for that LAN.

Note: The NTP server for a LAN could be located on a different LAN than the PCs. If so, select the UNIX server closest to the PCs' LAN.

A Network Time Policy needs to have been established at each site because this installation procedure does not prescribe a specific solution for synchronizing time on the UNIX servers. However, the following general practice may be appropriate.

PCs should synchronize with the closest UNIX server's NTP service. This probably is the UNIX server on the PC's LAN. If there is not a UNIX server on the PC's LAN, use the UNIX server on which the PC maintains its database.

One UNIX server on the WAN should be chosen as the secondary time standard for all EOCs. All other UNIX servers on the WAN should synchronize with that server.

The UNIX server chosen as the secondary time standard should acquire time synchronization from a primary time standard, via: 1) a local Global Positioning System (GPS) or WWV (NIST radio station broadcasting continuous time status) hardware clock, 2) stratum 1 host on the Internet, 3) dial-up modem connection to National Institute of Standards and Technology (NIST) using Automated Computer Time Service (ACTS) protocol, or 4) other as appropriate for each site.

Generally speaking, the options listed are in the order of decreasing reliability. Thus, the least reliable is local clock discipline, where no synchronization from an outside time standard exists. The most reliable methods are WWV radios and GPS. Synchronization via modem or Internet offers acceptable accuracy at modest cost.

Configuration scenarios for each method differ—however, the NTP service on the UNIX system receives its instructions via the configuration file at /etc/inet/ntp.conf. This file contains two important lines. One defines the path of the drift file. The other defines the server address or identifier of the source through which the NTP service on the UNIX system will obtain its time synchronization.

For more information on NTP, refer to the University of Delaware Web site on time synchronization: http://www.eecis.udel.edu/~ntp/. This page lists approximately 25 different drivers for clocks that can be interfaced directly to the Sun Solaris system.

Note: PNNL does not endorse any specific vendor or approach to establishing logical connections to time standard clocks, recognizing that sites have differing needs and topology constraints.

Whichever method for synchronizing time on the Sun server is chosen, please note that the hardware utilized must be fully compliant with NTP. Many ways are available to acquire time displays that are based on transmission from GPS, WWV, and NIST over modems. However, be careful with solutions that offer only proprietary data formats and interfacing methods, as these may not work as desired in an NTP environment.

This section of the SAG summarizes six clock disciplines.

12.1 NTP Synchronization Via Undisciplined Local Clock

This driver allows a machine to use its own system clock as the reference clock, with no outside clock discipline source. To establish a local clock, specify the following server directive in the ntp.conf file:

```
server 127.127.1.0
```

12.2 Synchronization Via NIST Modem Time Service

This driver supports the National Institute for Standards and Technology (NIST) Automated Computer Time Service (ACTS). It periodically dials a prespecified telephone number, receives the NIST timecode data, and calculates the local clock correction. It was designed primarily for use when neither a radio clock nor connectivity to Internet time servers is available. The available accuracy is within that which is required to operate FEMIS.

ACTS is located at NIST, Boulder, Colorado, and their telephone number is (303) 494-4774. Furthermore, a membership fee may be required. Refer to the Web site and modem vendor sources.

Required modem parameters are 1200 baud, 8-bits, no parity, Hayes compatible. The NIST ACTS telephone number and modem setup strings are hard-coded in this driver. If you need to change them, you need to acquire the source code, edit, and recompile.

To establish a NIST modem time service in the configuration file, use

```
server 127.127.18.u
```

where u is the port number on /dev/actsu.

12.3 NTP Synchronization Via Internet

FEMIS sites that have continuous access to Internet can configure NTP on their Sun computer to synchronize with any of about 50 time-standard clock servers on the Internet.

Set up the actual host you want to synchronize with by listing its domain name or IP address in a server directive in the ntp.conf file. Example:

```
server 192.43.244.18  # time.nist.gov       (recommended for west coast)
server 192.5.41.40    # tick.usno.navy.mil  (recommended for east coast)
```

For some EOCs, Internet time synchronization may be desirable because no additional hardware costs are involved once network access is already in place. Access to the primary time servers is free. The available accuracy is well within that which is required to operate FEMIS.

Using Internet to gain access to primary time servers has a potential network routing issue associated with it. NTP uses UDP port number 123. As a matter of policy, some sites block this specific access for security reasons. Sites considering NTP over Internet should study the security impacts. Many firewall components offer solutions to this problem. Also note that some routers support NTP internally. Call your network solutions vendor for specific advice.

12.4 NTP Synchronization Via WWV Radio Receivers

Many networking equipment manufacturers offer WWV radio-receiver-driven clocks that can be interfaced directly, via serial port, to the Sun computer and an NTP driver. Refer to the NTP Web site, and look for Reference Clock Drivers. This page lists about 5 to 10 different hardware solutions.

Note: Either WWV or GPS receivers are considerably more expensive than any of the previously mentioned methods. However, if accuracy and reliability are important, these methods offer substantial benefits and should be given serious consideration.

12.5 NTP Synchronization Via GPS Receivers

Many networking equipment manufacturers offer GPS-receiver-driven clocks that can be interfaced directly, via serial port, to the Sun computer and an NTP driver. Refer to the NTP Web site, and look for Reference Clock Drivers. This page lists about 5 to 10 different hardware solutions.

Note: GPS receivers for synchronization of NTP clocks are considerably more expensive than either modem or Internet methods. However, if accuracy and reliability are important, this method offers substantial benefit and should be given serious consideration.

Also, in some geographical locations, GPS may have a slight advantage over WWV radios, depending on the amount of high frequency radio interference present. Get the advice of radio installation consultants in your specific area.

12.6 NTP Synchronization Via Network Time Server

Vendors now offer both WWV and GPS Network Time Servers. These devices interface directly to your Ethernet via either 10Base-T or coaxial connections. Time synchronization signals are obtained either via WWV or GPS radio and antenna. These devices interface directly to the network and not through the computer's serial port. As such, they do not depend on specific computer hardware and operating systems for support. Possible vendors include TrueTime, Spectracom, Austron, Magnavox, Datum, and NMEA.

13.0 Security Measures

Security measures for the operating system and database are discussed in the following sections.

13.1 Operating System Security

Security measures in FEMIS include security goals, user account management, user identification number (UID) and group identification number (GID) management, password protection of accounts and files, other encryption, no access files, and NFS connections scripts. Consideration of factors common with EMIS operation on a PC or UNIX server has been taken into account.

13.1.1 FEMIS Operation System Security Goals

The goals of security measures taken for FEMIS include the following:

- Eliminate all passwords in the clear from NFS connection batch scripts.
- Accomplish Windows NT login and NFS connections via a single login dialog.
- Establish the unique UID number, login name, and secret password for each user in the EOC. Users will maintain their own passwords.
- Verify that server files created via NFS are owned by user's UID, and files created via NFS, while operating FEMIS, have GID femisrun.
- Verify that there is no access from ordinary user accounts to files on the UNIX server that might contain sensitive information.
- Verify that security measures are compatible with EMIS operations. Run FEMIS and EMIS on same PC. Run FEMIS and EMIS from the same login.

13.1.2 User Accounts

Each individual who uses FEMIS needs an account on the Windows NT workstation and UNIX server. For FEMIS, multiple accounts must be maintained on both NT and UNIX systems for security reasons.

Every person using the EOC computing resources needs a user account. If deemed suitable, an EOC's system administrator can create and maintain user accounts for each and every person who will be using a FEMIS workstation.

As an alternative, your System Administrator may want to set up groups of users rather than individuals. In that case, several people would use the same user name and password. Examples are setting up user accounts based on operating position in the EOC, e.g., safe for Public Safety or tran for Transportation.

13.1.3 UID and GID

The UID is a number that identifies user accounts in UNIX. Each user account, individual, or position must be assigned a unique UID. These numbers must be unique so that no two user names at the EOC will have the same UID. PNNL suggests using UIDs in the range from 100 to 60,000. The main use of UID is to establish ownership of files on the UNIX system.

The GID identifies group. Each and every user account created on a FEMIS UNIX server must be included in the femisrun group (30510).

During execution of FEMIS on a PC workstation, files created by that PC on M:\ and L:\ drives will have ownership/group userid/femisrun, where userid is the UID of the user account.

Files created by FEMIS workstations on M:\ include D2PC and Evacuation model log files and result files. If GroupWise is your E-mail application, it uses the L:\ drive.

At sites where both FEMIS and EMIS are being installed on the same server, the choice of UID and GID numbers should be coordinated with the EMIS vendor to ensure that these unique numbers do not overlap.

13.1.4 Passwords

A user or System Administrator must be concerned with two types of passwords, the Windows NT workstation password and that user's password on the FEMIS UNIX server. The Windows NT and UNIX passwords must be the same for FEMIS to work. If both EMIS and FEMIS are to be run from that user's PC, then they need to be concerned about the EMIS UNIX server password also.

Upon a FEMIS user logging onto a PC, the FEMIS startup script, FSTARTUP.EXE, is run from the Startup group. The result is network connections being made via NFS to the FEMIS UNIX server. Connections to drives M:\ and L:\ are established.

The users of FEMIS should be responsible for maintaining their own Windows NT login password and UNIX password(s). A user's UNIX account password must be identical to their Windows NT account password. That way, they only need to enter a password once, at the Windows NT Login Information dialog box. The password entered there will be reused for NFS connections needed in FSTARTUP.EXE. If NFS connection password authentication fails, FSTARTUP.EXE will prompt the user for his/her password(s).

Since a user's Windows NT and UNIX passwords must be the same, UNIX password rules (the more limiting of the two) must be used. Passwords must contain 1) six to eight characters, 2) at least two letters, and 3) at least one number. A password must differ from the user's login name or any circular shift of that name. Passwords must differ from the old password by at least three characters. Password uniqueness must be established in the first eight characters. Mismatches in characters beyond eight may-or-may-not be detected.

Each user (or group of users) is responsible for maintaining his/her own password. If password management is done by group, one person in that group should have prime responsibility for maintaining the password and letting it be known to others in that group.

Password maintenance on the PC is performed via Ctrl-Alt-Delete, which runs the Windows NT Security dialog box. Password maintenance of UNIX password is accomplished by running telnet to the UNIX server and using the passwd command for FEMIS and nispasswd for EMIS to modify passwords. Setting both passwords to the exact same string ensures that the password only needs to be entered once at the main Windows NT login window.

13.1.5 Encryption

Windows NT and UNIX account passwords are encrypted in the default methods of Windows NT and Sun Solaris operating systems. No other methods are incorporated in FEMIS for encrypting authentication passwords.

Data transmitted to and from the FEMIS command server are currently encrypted using a DES-like algorithm. A future version of FEMIS may use SSL. None of the other FEMIS daemons currently use encryption.

13.1.6 No Access Files

Some files in FEMIS may contain passwords or other sensitive information. These files have been made inaccessible to the normal EOC user accounts. This is accomplished by setting ownership/group to femis/femis and protection mask to 600 (rw-------), which results in no read access to the world. An example is the FEMIS Command Server configuration file. Do not change the protection to something else, e.g., 644, as then the world will be able to display and read the sensitive information contained in that file.

13.1.7 FEMIS/EMIS Issues

It is possible to run both EMIS and FEMIS on the same PC workstation and from the same Windows NT login. FEMIS uses drives M: and L: for access to a UNIX server. EMIS uses network drives N:\ and S:\ to access files on a UNIX server (may also use drive I:\ and T:\).

It is also possible to install and run both EMIS and FEMIS on the same UNIX server. Security models for UIDs, GIDs, and file ownership for the two systems are compatible.

Installations where both EMIS and FEMIS are supported on one or more UNIX servers will need user account maintenance in accordance with EMIS system administration.

Note: NIS+ is used in EMIS for maintaining user accounts. System administration policy regarding Solstice and NIS+ is discussed elsewhere in this manual.

13.2 Database Security

Most of the access security for previous versions of FEMIS has been provided by the client application. This was accomplished using the FEMIS usercodes and passwords and restricting knowledge of these to a minimal number of users at an EOC.

The FEMIS client application connects to an EOC database to access and share information with users in the same EOC and remote EOCs at the Hazard site. When a user starts the FEMIS application, a connection to the default EOC database is attempted using an Oracle userid and password that are saved in the application. If this connection is successful, the FEMIS Login window appears where the user enters a FEMIS usercode (Username) and password valid for the EOC where the user intends to work from. The FEMIS usercode and password are validated by comparing the values entered by the user with values in the database table, FEMIS_USER. If the usercode and passwords are correct, a database connection is made to the appropriate database and the application begins to initialize.

In previous versions of FEMIS, database userids and passwords for all EOC connections were stored in the EOC table with the password being encoded to prevent an unauthorized person to copy it. The database userid was derived from the EOC code and password was normally the same as the userid. These values were placed in the EOC table as part of the FEMIS installation or upgrade. There was no FEMIS interface to allow changes to the initial database passwords.
It is a long term goal to add more database security to prevent accidental or malicious access problems from occurring. The following increased security measures are included in this version of FEMIS:

- Increased access protection of the FEMIS relational database.
- Better relational database password management.
- New tool to change passwords.

13.2.1 Increased Access Protection for the Relational Database

In FEMIS v1.4.5, a single Oracle schema is provided for the management and access of an EOC's relational database. The initial authorization link to FEMIS, every access to Oracle by the FEMIS application, and all database administration work were executed by the same Oracle schema. This presented a database security issue in that authorized users are given more privileges than they need. A FEMIS user, using SQL, could inadvertently delete or modify an Oracle table needed by other FEMIS users which would damage the FEMIS system.

In FEMIS v1.4.6, additional Oracle schemas for each EOC's Oracle database exist for the following:

- The FEMIS "login" user – This initial access schema can only view part of a single table in the database. The password for this account is fixed and stored in the FEMIS initialization file, but the schema can only query parameters needed to perform the initial validation of a user's login.

- The FEMIS "application" user – This schema is used to access the FEMIS Oracle database from the FEMIS application after a successful login. This schema can view and edit data within the FEMIS database but does not have the ability to change the structure of the FEMIS Oracle tables or perform Oracle administrative functions.

- The management of the FEMIS relational database – This schema is used to create and manage the tables, indexes, procedures, and other objects of the database. This schema "owns" the production data and is used to complete all data administrative functions that are necessary.

- Two administration schemas for the UNIX login accounts – These schemas are used by AutoRecovery and other UNIX processes to access the local Oracle database. The password for each schema is identified externally to Oracle and is managed by UNIX, which provides security and change capabilities. These schemas match the UNIX femis and oracle user accounts.

13.2.2 Password Management for the Relational Database

In FEMIS v1.4.5, there are several security problems associated with the management of passwords used for accessing the FEMIS relational database. In several processes that use the database, passwords are stored in-the-clear, or they use a password which is the same as or derived from some well known string, e.g., EOC code. These processes include DEI, Setup, AutoRecovery, Command Server, Data Driven Notification (DDN), Shell scripts for database management, FSETUP.INI, FTP, and FPROFDEI. Because database passwords are being assumed and/or stored in the configuration they can be discovered by an experienced user.

Most of these processes have been modified to use the administration schemas. For example, AutoRecovery uses the oracle database administrator account to check the status of local and remote databases. DEI uses the femis database administrator account to put EMIS data into the database. To use either account, the process connects to the database using the slash (/) instead of a userid and password pair. Therefore, the password is not visible during the connection, and it may be changed frequently without any impact.

Some of the scripts for database management still retain the userid/password connection parameters. Most of these scripts are used when the database is initially installed or updated to a new version. After the database is installed or updated, the database passwords can be modified so they are different. If the scripts must be reused, a new tool is available to temporarily change the passwords.

13.2.3 Password Change Tool

Manage Database Passwords

The Manage Database Passwords tool is used to change the password for an application database schema or a management database schema. It can also be used to restore all owner schema passwords for the site to the installation default.

Warning: Before using this tool, be sure that all of the appropriate servers, databases, and networks are operating normally and that you know all of the necessary passwords to complete the operation. Also make sure the FEMIS ODBC data source names on the PC are correct and complete for all databases affected. If the environment is not complete or the passwords are not known, the process may only partially finish, requiring manual intervention from a System Administrator to appropriately restore the passwords.

In general, this tool is used as follows:

1. Select a DSN (the default upon entry is the DSN for your EOC).
2. Select one of the three available password options.
3. Enter the old and new passwords in the change schema password text boxes, if prompted.
4. Press the Execute button.
5. Respond to input requests.

Note: Remember that Oracle passwords are case sensitive.

Option 1: Change the Application Password

This option will change the password of the application database schema. This is the schema used by the FEMIS application itself. It has only the database privileges necessary for the execution of the FEMIS application and some of its utilities.

To change an application database schema password:

1. Select the DSN for which you wish to change the application database schema password from the Data Source Name drop-down list,.
2. Select the Change This Application Password option button.
3. Enter the current password in the Old Password text box.
4. Enter the new password in both of the New Password text boxes. The password must be between 4 and 16 characters in length and may only contain alphanumeric characters.
5. Press the Execute button. The process will run, changing the application schema password for the specified EOC.

Progress messages will appear in the process log text box. The last progress message will indicate whether or not the full process was successful.

6. Press the Clear Log button to reset the window, or the Close button to close the window.

Option 2: Change the Management Password

This option will change the password of the management database schema. This is the schema that owns the objects in the FEMIS database. Since this is the schema that owns and controls replication, changing this password involves all site servers.

To change an owner database schema password:

1. Select the DSN for which you wish to change the owner database schema password from the Data Source Name drop-down list.

2. Select the Change This Owner Password option button.

3. Enter the current password in the Old Password text box.

4. Enter the new password in both of the New Password text boxes. The password must be between 4 and 16 characters in length and may only contain alphanumeric characters.

5. Press the Execute button. The process will run, changing the owner schema password for the specified EOC.

   Progress messages will appear in the process log text box. The last progress message will indicate whether or not the full process was successful.

6. Press the Clear Log button to reset the window, or the Close button to close the window.

Option 3: Reset All Owner Passwords

This option will restore all owner schema passwords for the site to the installation default. It would typically be used only as part of an installation or upgrade process.

To reset all owner passwords:

1. Make sure that a Data Source Name (DSN) has been selected from the Data Source Name drop-down list. While all DSNs will be affected, one needs to be specified initially as the source for the basic EOC information.

2. Select the Reset All Owner Passwords option button.

3. Press the Execute button. The process will run, changing all owner schema passwords for the site to the installation default.

   If the current password for any given schema is not the default, you will get an Oracle login box for that schema. Enter the current password for that schema and press the OK button. If you do not know the correct password, the process will terminate.

   Progress messages will appear in the process log text box. The last progress message will indicate whether or not the full process was successful.

4. Press the Clear Log button to reset the window, or the Close button to close the window.

14.0 Backup Strategy for FEMIS

Backups are critical in the maintenance of your FEMIS UNIX server since they provide a safety net to prevent data loss in the event of disk failures, software, or operator error. Failure to properly backup your system can cause hours or days of unnecessary labor in reproducing lost files and configurations. The ideal backup strategy automates as much as possible, thus minimizing manual actions performed by the system administrator. However, an improperly implemented strategy can cause problems rather than protect data. If the recommendations outlined below need modifications for your system, please analyze the changes carefully to avoid problems.

This document provides a recommended backup strategy for the FEMIS system and supplies details on using scripts that are installed on the UNIX servers to automate the process and a procedure for implementing system backups on a Sun Solaris system.

14.1 Recommended Backup Strategy

Regularly scheduled file system and Oracle database backups are recommended in addition to manual backups done as part of system upgrades or planned hardware and software maintenance. The backup process should be automated to make sure it always gets done consistently. The best time to backup your system is during times of low use (usually during the night). A full file system backup followed by incremental backups (changed files) is recommended. This will ensure the system can be quickly restored with only a few tapes. A method of tracking taped backups and retention of the media will ensure your ability to recover from data loss.

Some of the data in the FEMIS Oracle database tends to accumulate and can lower performance if it is not periodically removed. If a historic copy of this data is desired, the data must be saved before it can be safely removed. Scripts that were installed during the installation of FEMIS can be used to perform these operations for meteorological (Met) data, D2PC case data, and journal log data.

The Oracle database backups and removal of historical data need to be coordinated with the file system backups. This ensures the saved database files are not in the process of being modified while they are being copied to tape, and old database files that are no longer needed on the disk can be removed after a successful tape image is made. If this old data is not removed, the disk can fill up in one to three weeks.

14.1.1 File System Backups

An automated strategy of running full file system backups once a week followed by incremental file system backups the other workdays is recommended. These file system backups must follow the database backups that occur the same night. After a successful full file system backup, the old Oracle export and log files created by the database can be removed.

This process should be repeated each week with different media. For example, at PNNL, we retain 6-months (26 weeks) of full backups and 2-months (8-weeks) of incremental backups. The tapes are numbered and designated as full or incremental backups and kept in numerical order in a cabinet. A

logbook is also used to track when tapes were used. The system administrator mounts the backup tape each night and then checks the next morning to ensure the backup ran successfully. If a failure of the media occurred, they can then rerun the backup manually. For disaster recovery, the latest full and incremental backups are kept in a different building. This backup regimen has proven to be highly successful in providing us with an efficient way to recover from data loss.

When the FEMIS software was installed on your UNIX server, files system backup scripts and template files were installed and are located in the install/backup_template directory. These scripts enable you to schedule and backup your file system. (See Section 14.1.2, File System Backup Procedures for the UNIX Server, to customize and setup the server for automated backups.) These files contain scripts that will check the full file system backup log for errors before removing the old Oracle export files. This prevents deleting these files without first successfully backing them up.

14.1.1.1 Full File System Backups

A full file system backup creates an image of your system and can be used to restore a disk to the point in time this backup occurred. The operating system tracks the occurrence of a full file system backup of each disk in the /etc/dumpdates file on your system. A full file system backup of a device is designated as a level 0 dump followed by the date and time it occurred, for example:

```
/dev/rdsk/c0t0d0s0    0 Sun Apr 12 00:00:52 1998
/dev/rdsk/c0t0d0s5    0 Sun Apr 12 00:06:04 1998
/dev/rdsk/c0t0d0s6    0 Sun Apr 12 00:11:22 1998
/dev/rdsk/c0t1d0s7    0 Sun Apr 12 00:33:28 1998
```

14.1.1.2 Incremental File System Backups

An incremental file system backup uses the data in the /etc/dumpdates file to determine which files have changed since the previous full file system backup and then writes only the changed files to tape. In order to completely restore a disk or directory, the full file system backup must be restored followed by the latest incremental. Incremental file system backups are designated by a level 9 dump in the /etc/dumpdates file.

14.1.2 File System Backup Procedures for the UNIX Server

Software backups and archiving are highly recommended as part of normal system administration operations and management. Example scripts are delivered to perform these tasks. The EOC and System Administrator should become familiar with the examples and make any modifications necessary to comply with their information system policies.

The backup files are located in the install/backup_template directory and include the following:

README.backup	
backup.sh -	The script which performs backups.
backup.sh.1 -	The backup.sh man page.
backup_system_full -	The control file template for full backups.
backup_full_data_file_1 -	The data file template for tape 1 of the full backup.
backup_full_data_file_2 -	The data file template for tape 2 of the full backup.
backup_system_inc -	The control file template for incremental backups.
backup_inc_data_file_1 -	The data file template for tape 1 of the incremental backup.
backup_check.sh -	The script to check for successful backups and call the Oracle export and archive log removal script.

To customize the backup templates for your site, complete the following steps:

1. Create the /apps/backup directory.

2. Copy the backup files to /apps/backup.

3. Configure the backup templates for the system. Each backup data file will write to one tape. If more than two full or one incremental backup tapes are required, create a new data file and add the new data file to the appropriate control file.

To run an Oracle archive removal script:

1. Uncomment the backup_check.sh line in the backup_system_full file.

2. Edit the backup_check.sh script to verify the EXPECTED_LOGS variable is accurate.

3. Modify the ORACLE_REMOVE variable to call the Oracle file removal script.

To run an automated backup, load the appropriate number of tapes and add the following to the root crontab:

```
#
#     Backups
#
35 0 * * 2 /apps/backup/backup_system_full > /dev/null 2>&1
30 0 * * 3-6 /apps/backup/backup_system_inc > /dev/null 2>&1
```

To perform backups manually, load the appropriate number of tapes and run the following commands.

Full backup (performed Monday evenings): # /apps/backup/backup_system_full &

Incremental backups (performed Tuesday-Friday evenings): # /apps/backup/backup_system_inc &

14.1.3 Oracle Database Backups

The Oracle database contains most of the information that is used throughout FEMIS. The database is a critical part of the system. To ensure the database can be restored in case of hardware malfunctions, software problems, or human error, it must be backed up on a regular basis. Although recovery may be complex depending on the types of damage to the database, it can usually be accomplished if the database was properly backed up.

To provide alternative methods of recovery, we recommend the following Oracle database backups be done.

Full database backups copy all the files that comprise the Oracle database. We recommend both periodic "cold" full database backups as described in Section 14.1.3.1, Cold Full Backups of the Oracle Database, and weekly "hot" full database backups as described in Section 14.1.3.2, Hot Full Backups of the Oracle Database.

Logical Oracle database backups are Oracle database exports. We recommend nightly logical Oracle database backups as described in detail in Section 14.1.3.3, Logical Backups of the Oracle Database.

Full database backups and logical database backups provide different recovery capabilities.

Full database backups are used to restore the Oracle database to any point in time, including the last time the database was operating normally. Please note that to recover using a full database backup, Oracle should be operated in archive mode so the archive logs are copied to a save area. To recover to a point in time, the last full backup files are loaded, and then the archive log files are applied until the desired point in time is reached. If archive log files are not available, a cold full database backup can still be used to restore the database to the point when the cold full database backup was made, but changes made after that time cannot be recovered. Recovery using a hot full database backup cannot be accomplished unless all archive logs are available.

Logical Oracle database backups are used to recover to the time when the logical database backup was completed. The Oracle import tool is used to regenerate the database in case of major failures. This type of recovery is useful to restore the database to a past state where the database was known to be good. If the database was damaged in some manner so that it would not start up, then imports would not be possible. In this case, the database would then have to be rebuilt using a complex process available in Oracle's installer, or the database could be restored from the most current set of files produced by a cold backup.

It is essential that the database backups be integrated with the file system backups. When this is done, the Oracle files will be ready to be copied to tape along with other disk files and disk space will be freed when old files are deleted after the successful file system backup. The system administrator should ensure the directory containing the archive logs, and the Oracle backup files are included in the file system backup.

When the FEMIS software was installed on your UNIX server, Oracle database backup scripts and template files were also added and are located in the oracle/admin directory. These scripts will enable you to schedule and automate backups for your Oracle database.

14.1.3.1 Cold Full Backups of the Oracle Database

The database must be shutdown to perform an Oracle cold full database backup. A script to perform a cold backup, named dbbackup_cold, is available in the oracle/admin directory. This script shuts down the database, copies the files to a save area indicated by the environment variable ORACLE_COLD and then restarts the database. In a multiserver configuration, shutting down the database on one server causes replication failures on remote servers since the remote servers continually try to query for database changes. Although these replication failures are temporary and are usually repaired when the database comes back up, sometimes more serious problems are encountered. Therefore, cold backups are not routinely used in FEMIS and are manually initiated at times when the database is shut down for other reasons. Database shutdowns should be coordinated with other remote servers to avoid complications.

Cold backups are recommended before the installation of a new FEMIS version and whenever the server is shutdown for several hours or more for maintenance. This backup can be used to restore the database to the specific date it was done. In addition, archived logs can then be applied to restore the database up to the time of the last archive if all archived logs since the last cold backup are available.

14.1.3.2 Hot Full Backups of the Oracle Database

Oracle hot backups are full backups that are done without shutting down the database. A script to perform a hot backup, named dbbackup_full, is available in the oracle/admin directory. This script first does a logical backup (see Section 14.1.3.3, Logical Backups of the Oracle Database) and then checks to see if the database is operating in archive mode. If the database is not in archive mode, a hot backup cannot be performed so the script exits. If the database is in archive mode, each data file is put into backup mode, and then it is copied to a save area indicated by the environment variable ORACLE_FULL. After that, the Oracle control file is copied to the same save area. At this point, the database is backed up, and the files in the save area can be copied to tape as part of the file system backup process. When all files are safely backed up to tape, the online Oracle redo logs are removed so the file space is available for the next set of logs.

It is recommended that hot backups be done weekly during off-use time when changes to the database are minimal. These backups can be used with the archive logs to restore the database to a point in time. All database archive logs, from the time the hot backup was started to the time of desired recovery, must be available in order to restore the database. If logs are missing, the hot backup will not succeed—for this reason, cold backups are considered essential.

14.1.3.3 Logical Backups of the Oracle Database

A logical Oracle database backup uses the Oracle export utility tool to make a consistent copy of the database to a file. A script to perform system level exports, named dbbackup_inc, is available in the oracle/admin directory. A system level export dumps all Oracle objects in all Oracle user accounts to the

save area indicated by the environment variable ORACLE_EXPORT. A typical logical backup takes about 5 minutes, and after this time, the export file is ready to be copied to tape by either a full or incremental file system backup. A logical Oracle database backup does not require the Oracle database to be shut down.

It is recommended that logical backups be done each working day during low use times to save the database as it exists. From this export, individual user accounts can be restored using the Oracle import tool. When this is done, data in all tables are restored to what existed at the time of the export.

Also, data in a specified set of tables can be restored from a logical Oracle database backup, leaving the rest of the database alone. This can be useful if data in a table is deleted accidentally because restoration to a previous day's logical Oracle database backup will save time by not having to recreate the lost data.

14.1.4 Removing Historical Met, D2PC, and Journal Log Data

As the FEMIS system is used, data accumulates in many of the Oracle tables. Certain tables may get extremely large and slow down the performance of the system. The Met, D2PC, and journal log data, all of which have frequent updates, are of special concern. Some sites wish to maintain a record of this information for an extended period of time, so the data cannot be deleted. Details of this process for each type of data is described in the paragraphs below.

Met data arrives at the Depot server about four times each hour and will add many records to the Met tables in a week's time. A script is available in the oracle/admin directory that will export the Met tables to the export save area indicated by the environment variable ORACLE_EXPORT. When the script, dbarchive_data, is called with a parameter indicating Met data, the Met_Tower, Met_Cluster, Met_Condition, and D2_Met_Met_Selection tables are exported. This exported data will be saved to tape when the next file system backup occurs. Then any Met data in these tables older than seven days is deleted from the table. It is recommended that the Met data is saved and removed automatically once a week by setting the script up as a cron job. This is only needed on the server where the Depot database resides.

The journal table is used to capture significant FEMIS changes such as event notification, data changes, acknowledgments of data received from other EOCs, and user journal entries. Depending on the extent of daily use of the FEMIS system, the journal table can become large. The same script described in the previous paragraph is called with a parameter indicating journal data to save and purge records in this table. We recommended the process be set up as a cron job to execute automatically once a month on all the servers.

Another process is available to manually archive Met and journal data with the user supplying interactive information to control the process. This process is available if the automated version described above fails or was not implemented. Instructions for using this manual process are in the Section 4.3.4, Archiving Tables, in the ***FEMIS Data Management Guide***.

Depending on conditions in the Emergency Operations Center (EOC), D2PC cases may accumulate over time and lower system performance. This is more likely to be a problem at the server where the Depot database resides, as D2PC cases arrive from EMIS periodically. A process is available to control the number of cases in the database. This process can be configured to operate automatically as a cron job, or it can be used interactively. Section 9.4.3, Archiving D2PC by Number of Cases, in the ***FEMIS Data Management Guide*** describes the process and the options available. It is recommended that the archiving of D2PC cases be tailored to your EOC and configured to operate automatically if D2PC case buildup is a concern.

14.2 System Backups for Sun Solaris System

The following is a procedure for implementing system backups on a Sun Solaris system using the PNNL developed backup.sh script and data files.

1. Create a directory on your Sun server to keep your backup logs and scripts. A commonly used location is /filesystem/apps/backup. You can add an entry to your /etc/auto_apps to automap this directory as /apps/backup.

```
# apps directory map for automounter
#
backup      -intr,rw,nosuid        system:/files0/apps/backup
```

2. Copy all files located in /home/femis/install/backup_template to your backup directory.

3. Document your system's configuration for the following items:

- Number of bytes that your tapes are able to store on your tape drive.
- Tape drive device address (e.g., /dev/rmt/#). If it is the only tape device on your system, it is likely to be /dev/rmt/0.
- Appropriate ufsdump options for your tape device (see the man pages on ufsdump and tape drive manufacture's specifications).
- Mount point of system disks.
- Disks size and bytes used.
- Document the directory where your oracle home account is located if you are going to remove Oracle exports after your full backup.

4. Configure each of the backup data files to match your system's configuration. Modify, if necessary, the following items:

- Options – This is the ufsdump options for your device. The template files are configured for 4mm DDS tape drives. The first option is for dump level and should be left as either 0 for a full backup or 9 for an incremental backup. You need to include the u and f options regardless of tape drive used.

- Device_file – This is the tape drive device address. If your tape drive can compress data, include the c parameter. Always include the n parameter (e.g., /dev/rmt/#cn).

- Filesystem – This is the mount points of the system disks (space delimited). Your typical incremental backup will include all file systems. Most full backups will need two or more full data files. Do your best to arrange them so tapes do not run out of space. Do not duplicate or leave out any disk drives.

- Mail_to – This is a list of UNIX accounts or E-mail addresses (space delimited) which will receive the backup log and a warning list at the end of the each backup tape.

5. Each backup data file will write to one tape. If you need more than two full or one incremental backup data files, make a copy of an existing file and name it according to the order it will be used. Edit and change the log_file option to match the data file number.

6. Add/remove lines in the backup_system_full and backup_system_inc files so they execute all the data files with the backup.sh script. Be sure a sleep 360 command separates each backup execution for autoloaders. This command gives the tape drive time to unmount and remount the tapes.

7. To run an Oracle archive removal script, uncomment the backup_check.sh line in the backup_system_full file. You will also need to edit these variables in the backup_check.sh script:

   - ORACLE_REMOVE – This line will be oracle_home_directory/admin/dbbackup_cron –clean.

   - EXPECTED_LOGS – This will be the number of backup logs generated by the full backup.

   - LOG_PATH – The directory where these logs are located.

   When this script runs, it mails its results to the root mail account by default. The E-mail account can be changed by editing the backup_check.sh script. Modify the following section (near the bottom) by replacing root with the E- mail account you want to receive the results.

```
if [ -f "$LOG" ];
 then
  < $LOG mailx -s "Oracle Export Removal $REMOVAL_STATUS " root
  rm $LOG
fi
```

8. To run an automated backup, load the appropriate number of tapes each night and add the following to the root crontab:

```
#
#     Backups
#
35 0 * * 2 /apps/backup/backup_system_full > /dev/null 2>&1
30 0 * * 3-6 /apps/backup/backup_system_inc > /dev/null 2>&1
```

   This entry in the root cron will execute a full backup at 12:35am Tuesdays and incremental backups Wednesday through Saturday at 12:30am. To perform backups manually, load the appropriate number of tapes and run the following commands as root.

   Full backup command: `# /apps/backup/backup_system_full &`

   Incremental backup command: `# /apps/backup/backup_system_inc &`

9. Label and date your tapes.

10. Do not reuse the same tape for each backup. You should keep several good tape backups on hand at all times. Determine how long you want to retain full and incremental backups and purchase sufficient tapes to cover that time. You should also purchase extra tapes to be able to replace bad tapes. Your full backups should be kept significantly longer than incremental backups and keep full backups separate from your incremental backups. Mount the oldest incremental or full tape each time backups run.

15.0 FEMIS UNIX Server

The FEMIS UNIX server software provides notification between servers, the transfer of data between FEMIS and EMIS, the capability to gather meteorological data, and the ability for PCs to use the server resources for large mathematical model/simulation codes. The software on the UNIX server consists of the FEMIS host Notification Service, the FEMIS command server, the FEMIS Met application suite, and the FEMIS Data Exchange Interface (DEI). These services, combined with the UNIX COTS applications, provide the structure for the FEMIS software.

15.1 Maintenance of the FEMIS UNIX Server

Consistent server maintenance is essential for FEMIS operation. The following steps should be taken regularly to monitor and maintain the server.

15.1.1 Monitor Oracle and FEMIS

The UNIX FEMIS Monitor and/or FEMIS AutoRecovery can be used to monitor critical FEMIS functions. These functions include the FEMIS Notification Service, the FEMIS Command Server, the FEMIS DEI, the number of Oracle PC connections, the Oracle Listener, and Oracle replication. For more information on the FEMIS Monitor, see Section 2.0, FEMIS Monitoring Tools, and for Oracle maintenance, see Section 14.1.3, Oracle Database Backups.

15.1.2 Perform System Backups

System backups are critical to data recovery. It is highly recommended that each EOC establish backup procedures. For more information on Oracle backups, see Section 14.1.3, Oracle Database Backups, and for server backups, see Section 14.1.1, Full File System Backups.

15.2 Troubleshooting the FEMIS UNIX Server

The following items are provided for the System Administrator to aid in the administration of FEMIS. For more information on the COTS products, please refer to the documentation provided by the vendor.

15.2.1 FEMIS Troubleshooting

If FEMIS processes are down the following commands may be used to stop and restart all FEMIS processes.

```
# sh /etc/init.d/femis stop
# sh /etc/init.d/femis start
```

15.2.2 Oracle Troubleshooting

In the event of an abnormal server shutdown, while attempting to start, the Oracle Listener may return an error similar to "Network name not unique on network."

To resolve the problem, remove the /var/tmp/o/s<SID> file and restart the listener.

15.2.3 NFS Maestro Daemon

PCs may receive the following error when trying to connect to the server.

Network Timeout or HCLNFSD/PCNFSD not running on Host.

This error message typically occurs for one of the following reasons:

1. The mountd daemon is not running on the UNIX server. To resolve, start the mountd daemon.

   # sh /etc/init.d/nfs.server start

2. The HCLNFSD daemon is not running on the UNIX server.

3. The NFS locking daemon is hung on the UNIX server.

For steps 2 and 3, stop the NFS Maestro daemon, if it is running.

sh /etc/init.d/hclnfsd stop

Restart the daemon

sh /etc/init.d/hclnfsd start

If the error continues, you may need to stop and restart the server locking daemon. Stop the NFS Maestro daemon, if it is running.

sh /etc/init.d/hclnfsd stop

Stop lockd

sh /etc/init.d/nfs.client stop

Restart lockd

sh /etc/init.d/nfs.client start

Restart the NFS Maestro daemon

```
# sh /etc/init.d/hclnfs start
```

16.0 FEMIS PC Utilities

The FEMIS PC utilities include the following programs:

FSTARTUP
WINECHO
FIXINI
SRVCTL
WRITEREG
WRITEINI
MSGBOX
AUTOEXNT
NTPQ
NTPDATE

16.1 FSTARTUP

FSTARTUP.EXE is the FEMIS startup script. It should be set to run automatically each time a user logs into Windows NT. It maps network drives and runs startup scripts specified in the %windir%\FEMIS.INI file.

For each entry in the [FemisPC] section of FEMIS.INI of the form

XDriveNetPath=<network path>

FSTARTUP.EXE will attempt to connect drive X:\ to the network path specified where X:\ can be any drive letter. It will attempt to make the connection using the Windows NT login username and password.

FSTARTUP.EXE also looks for the entries

LocalStartupScript=<filename>
EMIS_StartupScript=<filename>

Where filename specifies the full path to a file. FSTARTUP.EXE will attempt to run files specified in these two entries.

16.2 WINECHO

This program is for use by NT-DOS batch files running under Windows NT and allows a batch file to give a message to the user in a normal Windows message box. This utility is used by several batch files and the setup program.

Usage:

WINECHO message text.
WINECHO [/Beep] [/Info] [/Warn] [/Stop] /Msg:message text.

Parameters:

/Beep	Beep the speaker
/Info	Use the information icon in the message box
/Warn	Use the warning icon in the message box
/Stop	Use the stop icon in the message box
/Msg:	Any text following /Msg: will be shown in the message box. If any other parameters (/Beep, /Info) are specified, then /Msg: must be specified.

16.3 FIXINI

This program "fixes" the FEMIS.INI file by determining the PC name and setting the correct paths and filenames for some of the COTS packages used by FEMIS. The COTS that FIXINI.EXE will search for include the following:

ArcView GIS	
E-mail package.	FIXINI.EXE will search for Novel GroupWise, Microsoft Outlook, and Eudora. If more than one of these is found, FIXINI.EXE will prompt the user to select the package to be used by FEMIS.

This utility is called by the FEMIS Setup program. If any command line parameters are specified, then the program will exit immediately after writing information to FEMIS.INI. Otherwise, it will wait for the user to click OK.

16.4 SRVCTL

This program allows starting and stopping of Windows NT services from the command line. This program is used by the setup program to start the NTP service to synchronize the PC's time with the server.

Usage:

-s ServiceName	Starts service "ServiceName"
-e ServiceName	Stops service "ServiceName"

Note: The ServiceName passed is case sensitive. It must be entered exactly as it appears in the Control Panel.

16.5 WRITEREG

Write a value into the Registry. This is used by several batch files to add the correct ODBC information for FEMIS users.

Usage:

```
WRITEREG [/?] [/Q] [/D] /T:'type' /R:'registry' [/N:'itemname'] /V:'value'
```

Parameters:

/? = Help message.
/Q = Quiet mode-no status messages.
/D = Delete entry (/V parameter not needed for delete).
/T:'x' = Registry type.
R = HKEY_CLASSES_ROOT
C = HKEY_CURRENT_USER
M = HKEY_LOCAL_MACHINE
U = HKEY_USERS
/R:'x' = Registry entry.
/N:'x' = Value Name.
/V:'x' = Value to set.

If a value begins with '#', it is written as a DWORD value, otherwise it is treated as a string value.

Note: Values 'x' must be within apostrophes if the value contains a space, otherwise the apostrophes are not needed.

Example:

```
WRITEREG /T:C /R:'Software\ODBC\ODBC.INI\XXXX' /N:Server /V:FI_XXXX
```

16.6 WRITEINI

Write a value into an INI file. This is used by several batch files to add the correct ODBC information for FEMIS users.

Usage:

```
WRITEINI [/?] [/Q] /F:'file' /S:'section' /I:'item' [/V:'value']
```

Parameters:

/? = Help message.
/Q = Quiet mode--no status messages.
/F:'x' = INI filename to use.
/S:'x' = Section name in INI file.
/I:'x' = Item (key) in INI file.
/V:'x' = Value to set. (No value = Delete entry)

Note: Values 'x' must be within apostrophes if the value contains a space, otherwise the apostrophes are not needed.

Example:

```
WRITEINI /F:'FEMIS.INI' /S:'FemisPC' /I:'FemisUserTopDirUNIX' /V:'/home/femis/user'
```

16.7 MSGBOX

MSGBOX gives a Windows message box to the user. This allows the batch file to determine which button the user clicked so it may skip some steps. This is not used by any FEMIS batch files at this time, but may be used by FUPDATE.BAT files at some FEMIS sites.

Usage:

```
MSGBOX [/?] [/BTN:x] [/ICO:x] /M:'message' [/T:'title']
```

Parameters:

```
/?      = Help message.
/M:'x'  = Message to show the user.
/T:'x'  = Title of message box window.     (Default = 'Message')
/BTN:'x' = Button combination to show user.  (Default = OK)
           OC  = OK & Cancel buttons
           YN  = Yes & No buttons
           YNC = Yes & No & Cancel buttons
         The button clicked can be determined by the ERRORLEVEL.
           OK,YES = 0
           NO     = 1
           CANCEL = 2
/ICO:'x' = Icon to show in message box.     (Default = No icon.)
           Q = Question
           I = Information
           E = Exclamation
           S = Stop
```

Note: Values 'x' must be within apostrophes if the value contains a space, otherwise the apostrophes are not needed.

Example:

```
MSGBOX /M:'Update your GIS data now? This could take several minutes to copy.' /BTN:YN
/ICO:Q
    IF ERRORLEVEL==1 GOTO LABEL_SKIP_COPYING
      ::**(Copy files)
    :LABEL_SKIP_COPYING
```

16.8 AUTOEXNT

AUTOEXNT is public domain software written by Jan van Eekeren (janveeke@microsoft.com). The version of this software, installed with FEMIS, was obtained from the Microsoft Windows NT Resource Kit CD. The zip file for this software also is available via the Internet.

The purpose of AUTOEXNT is to automatically run a batch script at boot up time. The AUTOEXNT.BAT batch script is run only once per cold boot of the PC. AUTOEXNT is installed as an automatic service in the Windows NT Control Panel.

In FEMIS v1.4.6, the purpose of AUTOEXNT is to automatically set the PC's internal clock using the NTP utility program NTPDATE.

16.9 NTPQ

NTPQ is the NTP query program that queries the NTP servers on the network. NTPQ is installed both on the FEMIS UNIX server and on PCs. Useful reports can be obtained using the following commands:

```
>> ntpq -p
>> ntpq -p -n
```

The listing displayed shows the name or IP address of each NTP server on the network, the type of reference clock at each server, time correction statistics for each server, and from which server the client currently is acquiring synchronization (line with asterisk).

Example:

```
>> ntpq -p
remote           refid      st t when poll reach   delay   offset  disp
napoleon.eoc.org r11.eoc.org 3 u  487  1024  77     15.27   38.875  21.88
*wwvradio.eoc.org .WWVB.    1 u  233  1024  377    0.00    42.457  27.34
```

For a detailed description of the fields displayed by NTPQ, refer to the man pages. On any web browser, open http://www.eecis.udel.edu/~ntp/. Field st is the stratum number. The when and poll show when the server will again be polled. The when number increases once each second. When reaches poll, the client polls the server. The value of poll starts at 64 (about 1 minute) and increases up to 1024 (about 17 minutes). The numbers represent the adjustments.

16.10 NTPDATE

NTPDATE is the NTP set date program that can be used with cron to implement time adjustments. However, it is usually used to make a preemptive adjustment to the PC's internal time of day clock. The single argument to NTPDATE is the NTP server's name or IP address. NTPDATE is available both on UNIX server and on PCs.

To use NTPDATE, you must be logged in as root on the UNIX server or as Administrator on the PC. To run NTPDATE, the NTP service must not be active, as there can be only one user of the NTP port (IP service port number 123) at a time. On Windows NT, the -b option is required.

Example:

```
>> ntpdate -b napoleon
15 Oct 11:50:05 ntpdate: step time server 13.2.8.43 offset 0.005444 sec
```

16.11 INSTSRV

This program is used to install Windows NT services from the command line.

Usage:

instsrv <service name> <exe location>
to install a service, or:
instsrv <service name> remove
to remove a service
instsrv <service name> query
to query a service configuration

16.12 SWITCHDB

This program is used to change the default database that FEMIS connects to and to attach the FEMIS planning database. This program is accessible from Start → Programs → FEMIS → Change Default Database.

Note: After selecting a database and clicking OK, the OK button remains enabled. Clicking on OK while the planning database is being attached will restart the attach process. This will not cause any problems, but it will generate several messages stating that certain tables have already been attached.

16.13 FUNITCVT

This program provides users an easy method of converting units for temperature, weight, length, area, volume, speed, and pressure. This is a Windows NT application.

16.14 Stand-Alone Watchful Eye

The Stand-Alone Watchful Eye is an application that allows FEMIS users to be notified when an event occurs or other important decisions are made. The main use of this application is so users can monitor events without having to run the FEMIS application, which consumes significant PC resources. The user registers interests in specific events. When an event of interest occurs, the Watchful Eye responds according to the user's preferences. The user may then start the FEMIS application to obtain the details for the event.

16.15 Remote Evacuee Registration

The Remote Evacuee Registration (RER) application will provide users with the capability to enter evacuee information from shelters during emergencies. The user does not need to be connected to the network in order to use the application. A dialup connection to the server can be established via a modem link whereby the evacuee information can be uploaded on request. This offers the convenience of being able to register evacuees from remote locations via a laptop and other portable PC. Use Point-To-Point Protocol (PPP) to establish a modem link.

The RER application is installed as a part of the standard FEMIS installation process.

17.0 FEMIS Application Error Messages and Troubleshooting

This section contains error messages along with the possible solution(s) to the error, and troubleshooting of common problems with a possible resolution. ***The error message is denoted by bold and italics within quotes.*** In any situation below, that cannot be resolved with the solution(s) indicated, it is recommended that you contact the FEMIS Help Desk for assistance. This section only covers problems noted within the FEMIS application. For AutoRecovery error messages and troubleshooting, see Section 10.5, AutoRecovery Troubleshooting, in the SAG.

17.1 Application Error Messages

This section is in alphabetical order via error messages.

"Can't connect to GIS – gdaSymb_getObject. 380: Invalid property value."
This message displays after the user has invoked the object version of Select Location from the operational task status board, cleared the selections from all three drop-down lists, and clicked on the Map button. You should

- Select a specific location type before clicking the Select button that invokes the GIS.

"Can't start RCP server"
If you receive this error when attempting to log into FEMIS after a Windows NT v4.0 installation, contact the IEM's FEMIS Help Desk for assistance.

"Dr. Watson Errors"
When a specific window in FEMIS does not work on one PC (usually it will give a Dr. Watson), but the window works fine on other PCs. You should

- Verify if another software program was installed after FEMIS. It is possible that a file was overwritten that is used by FEMIS. This file may be different and an incompatible version compared to the one installed by FEMIS. In this case, run the FEMISCHK program on both a PC that works and the PC that does not work to see if there are any differences. If there are differences, copy the changed file(s) from the PC that works to the one that does not work.
- Check to see if these applications are attempting to start unexplainably. When you logon to Windows NT, you might receive a Dr. Watson error relating to KeyPrint or other executables that may not be in the start-up group, such as D2PC. The outcome is that the login is successful, but KeyPrint or the other application is not on the task bar. To fix this problem, you should enter Explorer, go to Winnt → Profiles → All Users → Start Menu → Programs → Startup (this should be the location for the KeyPrint and other application Shortcuts). In the right half of the Explorer window, right click on application needed, then select Properties → Shortcut tab. Make sure Target field contains C:\FEMIS\<application name>. If it does not, manually type it in.

"Error Creating Temporary Working Database"
This error indicates a problem with the Access database on the PC being used. The problem can arise for many different reasons. You should

- Logout of FEMIS on the PC, and delete the directory C:\FEMIS\USER\<user>\ETC where <user> is the username of the person having the problem on the PC. You can also delete all the directories under C:\FEMIS\USER if other files have not been stored there.

"Error selecting objects from GIS: Unknown error and the GIS displays: Status Unknown Error"
This error occurs when the location is a zone, but it does not occur if the location is a point theme. The error message is displayed if the user clicks the View button when displaying the details of a task in the Task Status Board.

- Click OK on the error message and continue. The error message does not cause any problems within FEMIS.

"Error writing user preferences to Database, 75:Path/File access error"
This error indicates a file protection problem on the M:\ drive connection. You should

- Save some arbitrary file to your M:\ drive. Telnet into the server, and move to the location pointed to by the M:\ drive. In general, this should be /home/femis/user. Check that the file you just saved is in the femisrun group and that the protection is at least 775. If it is not in the femisrun group or you could not save the file at all, verify that your UNIX account is in the femisrun group.
- Check if the /home/femis/user/<user name>/femisusr.ini file has some protections that would not allow another user in the femisrun group to overwrite it. If this is the case, there is probably another PC account incorrectly configured that saved the file in the first place.

"Error determining if an event is in progress"
If this error message is displayed, you should check with your System Administrator and verify that the Oracle database is still running. If not, your System Administrator should restart the database.

"Error opening project. 429: ActiveX component can't create object"
MS Project must be brought up once after being installed or it will not work properly within FEMIS. This error occurs when MS Project has not been opened via Window NT. You should open MS Project through Windows NT, not FEMIS, then close it. MS Project should now function correctly.

"OLE Error" when reading the database
This error occurs when you are only able to run the electronic plan from the default EOC. If you are logged into the correct default EOC, you must have an Access Database "attached" to the Oracle database. You should

- Check the Current Info item under the Help menu bar to ensure you are logged into your default EOC. If not, log in to the correct EOC.
- Run the Change Default Database program to correctly attach to the default database. This process is only done once when you define the default EOC to be connected to the PC.

***"OLE 40"* error**

This error will display if the C:\FEMIS\GLOBAL.MPT file is not copied to C:\WINPROJ. You should request that your System Administrator copy the correct GLOBAL.MPT file to C:\FEMIS.

"PARDOS Error Condition; No output available"

In some circumstances, the message can be encountered.

- PARDOS will not run but is not blocked. Save the case and contact IEM's FEMIS Help Desk for assistance.

"Run Time error '401' can't show non-modal form when modal form is displayed."

This error occurs when a message is hidden behind the GIS or another FEMIS window.

- Click OK and proceed. The hidden messages should come to the front of the GIS or other FEMIS window.

"The D2PC run cannot be logged"

If this error message occurs, the system is unable to log D2PC information to the M:\ drive. You should check the following:

- Verify that the FEMIS.INI file is pointing to the proper place on the server to log D2PC runs. This file should be on the M:\ drive. Verify the FEMIS User top directory NFS item is in the [FEMISPC] section.
- Verify that the PC is connected properly to the server (if there is no M:\ drive) during startup. The M:\ drive should be properly connected; if not, disconnect and reconnect to the correct path. Verify, even if the PC or the user on this PC never connects, that they are running the BATCHES.BAT script, see Section 4.4.1, Setting Up FEMIS User Accounts on NT and UNIX, in the ***FEMIS Installation Guide.***
- Verify you have the proper privileges on the UNIX server to log the D2PC case.

"Unable to Connect to the Oracle Database"

If FEMIS is unable to connect to the Oracle database on a single PC, but other PCs connecting to the same server are working correctly, the problem may be with the PC or the network connection to the single PC. Try one or all of the following:

- Log out of Windows NT and log back in. In most cases, FEMIS will now run correctly.
- Shutdown the PC, and verify that the network cable is connected. If you have the equipment, check that the network cable is "live." Reboot and try again.
- Run the FEMISCHK program on both a PC that works and the PC not working to see if there are any differences. If there are differences, you can copy the changed file(s) from the PC that works to the one that does not work. The FEMISCHK program is located on C:\.
- Reinstall the FEMIS configuration files (e.g., ODBC.INI, TNSNAMES.ORA). Run the Setup program, and select the Only Configuration Files option. Reboot and try again.
- As a last resort, completely reinstall FEMIS. Run the Setup program, and select the Full Installation option. Reboot and try again.

If all PCs start getting the Oracle error at the same time, it is either a problem with the UNIX server, the Oracle database, the Oracle listener, or the network. You should

- Try running C:\FEMIS\TOOLS\FMONPC.EXE, and select Check Server Programs to see if this PC can connect to any other databases. If they cannot connect at this point, contact the IEM's FEMIS Help Desk for assistance.

"Unable to establish notification link with <server name> in 10 seconds"
If you receives this message, it could be because the server or network is experiencing problems. You should verify the following:

- The UNIX server may be down. Check the server and restart it, if necessary.
- From the server, run the command ps -ef | grep femis_event. This should return a list of all the femis_event daemon processes currently running on your server. There should be one notification process running for each EOC database on your server. If there are not or you would like to simply restart them, you can restart notification from the femis UNIX account by issuing the stopnotify followed by the startnotify commands.
- The Notification server name or port number may not be valid. Check the EOC table in your FEMIS database and make sure the Notification server name and port number are correct.
- The network is down or unusually busy. Run the FWATCH program to verify network and server status. Tell FEMIS to keep trying to connect with the Notification server, or close FEMIS and try again.
- If the problem persists, your System Administrator may need to increase the MaxSocketWait value in your notification configuration file.

"Where is ...MIS\GIS\<SITE NAME>\FACILITY\E0\FACILITY.DBF or FACILITY.SHP?"
This message may display when you are installing the GIS. Having existing GIS ViewMarks can cause the message to display.

- Click on Cancel All.

"Your clock may be configured incorrectly"
If you receive this message when clicking the Now button in Event Declare, Work Plan, or Status Boards, then the clock is probably not configured correctly. You should

- Go to the Windows NT Control Panel, and verify that your PC clock is setup correctly. See Section 4.1.1, Installing Windows NT v4.0, in the ***FEMIS Installation Guide***.

17.2 Troubleshooting

This section contains information necessary to help troubleshoot common problems. In any situation below, that cannot be resolved as indicated, it is recommended that you contact the FEMIS Help Desk for assistance.

☐ AutoD2PC Result Graph does not Display

If the D2PC Result Graph window does not display properly and where the bar graph should display the window behind AutoD2PC shows instead, there is a problem with the Graphics Server program distributed with FEMIS.

- Delete the files GSW32.EXE and GSWDLL32.DLL from the %WINDIR%\SYSTEM32\ directory on the PC.
- Recopy these files from /home/femis/pc/system directory on the server to the %WINDIR%\SYSTEM32 directory on the affected PC.
- Shutdown and restart the PC.

☐ Database Performance Issues

If your site is experiencing performance problem, one cause may be the number of exercises. It is recommended that your System Administrator examine the number of exercises currently in the database. Excessive exercises in the database can affect performance for all modes. It is recommended that the total number of exercises be kept to a minimum and that the exercises be deleted when they become obsolete. Refer to the FEMIS Help on deletion of exercises.

☐ E-mail Notification does not Display

If you are not receiving E-mail notifications within FEMIS, you should

- Check to see if you can access mail directly from the E-mail application. If direct access did not work, your account may not be valid and should be added to the E-mail application. Check with your System Administrator for account information.

☐ Facilities in the Database Appear Different Between EOCs

If you are experiencing a problem where (depending on which EOC you are logged in to) you get different lists of the facilities in the database (even though the GIS looks the same for all of them), the problem is the file protections on the facility.evt file have been set to Read-only. This causes the facility theme not to be regenerated in the GIS when you change mode. You should request that your System Administrator change the appropriate file permissions.

☐ GIS Troubleshooting

The MAP button on the FEMIS menu bar is grayed out. This implies 1) ArcView GIS has not been installed, 2) ArcView GIS or other COTS were installed after the FEMIS installation, or 3) the path provided in the FEMIS.INI file to access the ArcView GIS executable is incorrect.

- Reinstall ArcView GIS (see Section 4.1.4, Installing ArcView GIS v3.0 and v3.01 Patch, in the *FEMIS Installation Guide*).
- Run C:\FEMIS\FIXINI.EXE to fix the paths to these programs.

ArcView GIS runs, but it keeps asking where files are and putting up a directory window. This implies that the data provided in the FEMIS install was not properly copied to the GIS directory.

- Make sure **all** of the FEMIS GIS files and directories are copied down to each PC, by running the FEMIS Install programs. Contact IEM's FEMIS Help Desk for assistance.

ArcView GIS gives other errors when starting.

- If the GIS EXE entry in the [FEMIS COTS] section of the FEMIS.INI file contains ...\BIN\ARCVIEW.EXE or ...\BIN16\ARCVIEW.EXE, go to the specified directory and rename ARCVIEW.EXE in that directory path to ARCVIEW2.EXE. Then rerun C:\FEMIS\FIXINI.EXE. You may also have to rerun the FEMIS SETUPGIS.EXE program to have the FEMISGIS.APR file created correctly.

If the following message ***"...can't close the GIS while in debug mode..."*** displays, it indicates that an error has occurred in a previous step.

- Close the GIS program using the Windows NT Task Manager. If this process does not work, logoff from Windows NT.

☐ Help Links Appear Disabled

If you are in Help and your hypertext links are not green, the problem could be with how your colors are set up and displayed on your PC. The links will still work.

- If you have this problem, check with your System Administrator to change the display setup.

☐ Login Troubleshooting

If the FEMIS Login window does not work for any reason, review Section 4.3, Installing FEMIS Client Software, in the ***FEMIS Installation Guide*** to verify that all of the installation steps have been completed. The following is a list of the most common items to verify.

- Verify the EOC table in the database has been updated to include the name of your server. To update, see Section 2.3.6, Configuring the FEMIS Files, in the ***FEMIS Installation Guide***.
- Verify the FEMIS database Listener is active. If not, start the Listener.
- Verify that the TNSNAMES file has been moved to the C:\ORANT\NETWORK\ADMIN directory. If not, move the correct TNSNAMES to the C:\ORANT\NETWORK\ADMIN.
- Verify that the usercode/password is valid. Check with your System Administrator to set up a new usercode/password.
- Verify that the ODBC data source has the proper connection information.
- Verify that the system is pointing to the correct default EOC. Rerun Change Default Database to identify the default EOC for your PC.

- Verify that the FEMIS Command Line and Working Directory are correct. Right click on the FEMIS icon on the Windows NT desktop, and select Properties. Select the Shortcut tab, and ensure that the target is set to C:\FEMIS\FEMIS.EXE and Start in is set to C:\FEMIS.
- FEMIS will log error messages as they occur on each PC, so you will see the error messages received. Examples:

ErrorLevel = 0 -- Bad errors. always written to M:\ERROR.LOG
ErrorLevel = 1 -- Status info. written to M:\STATUS.LOG if M:\ERRLEVEL.1 exists.
ErrorLevel = 2 -- Application errors. written to M:\FEMISERR.LOG if M:\ERRLEVEL.2 exists.

☐ **Menu Items Grayed Out**

If a FEMIS menu item is grayed out, it can be for many reasons. You should check the following items:

- Verify that a mode has been selected on the Navigator. Many FEMIS menu items are unavailable until a mode has been selected.
- Verify that you have the appropriate privileges. If not, contact your System Administrator to assign the appropriate privileges.

☐ **No Data or Outdated Met Information**

If there is no data or outdated Met information, the EMIS/FEMIS interface may not be properly installed.

- Refer to Section 7.0, FEMIS Data Exchange Interface (DEI).

☐ **ODBC Troubleshooting**

In ODBC Administrator, a newly added EOC data source do not show up in the list; yet when trying to add one, it said the data source already exists. If you attempt to add a completely different one, it may seem to accept it, but it still did not show up in the list in the Administrator window. You can still see and connect to all of the data sources via the ODBC Test utility and could select and connect to any of the EOCs just fine through FEMIS or the Change Default Database utility. However, you cannot connect to any of the EOC databases in ArcView GIS. The fix is as follows:

- Click on Start → Run, type in regedt32, and click OK (this is the Windows NT Registry editor). **BE VERY CAREFUL WHEN EDITING THE REGISTRY!!**
- Go to the HKEY_CURRENT_USER window, and click on Software → ODBC → ODBC.INI → ODBC Data Sources.
- Scroll through the list of entries until you find one beginning with <NO_NAME> or <NONE>. If you do not find one, exit the NT Registry editor because something else is causing your problem. If you found one, click on it to highlight it, and delete it (select the Delete option from the Edit menu). If there are more than one of these entries, delete all of them.
- Exit the NT Registry editor (select the Exit option from the Registry menu).

☐ Printer Troubleshooting

GIS printouts are not readable. You should

- Attempt to change the default colors on the PC.
- Contact your System Administrator for assistance.
- Try using KeyPrint to print the GIS printout.

☐ Tracking Navigator is Gray or Empty

When viewing data from other EOCs, the Tracking Navigator window is gray and empty or error messages appear in the Tracking Navigator cells. Check the following items:

- Verify the databases at the effected EOC are active.
- Verify the Oracle Replication functionality is working properly.
- Verify that you have the appropriate privileges. If not, contact your System Administrator to assign the appropriate privileges for you.
- Verify that data has been added to the other EOCs.
- Verify you are not in a "private" exercise that does not exist on the other EOCS.

☐ Tracking Navigator Text does not Display Correctly

If the text does not display correctly in the Function boxes on the Tracking Navigator, try the following:

- Run the following command: REGSVR32 OLEPRO32.DLL, and reboot the PC.
- Run the following commands, if the above command did not fix the problem, and reboot your PC.
  CD %WINDIR%\SYSTEM32
  FOR %F IN (*.DLL) DO REGSVR32 /S %F

☐ Site Defined Status Boards Troubleshooting

There are no names in the Status Board Name field. You should

- Verify that Site Defined Status Boards have not been generated.
- Verify you have privileges set for that Status Board.