GOV PROGRAM(GOV PROGRAM)
GOV PROGRAM (GOV PROGRAM)

LOGO REMOVED

System & Database Administrator's Manual
(DRAFT)

NO CLASSIFICATION ASSIGNED

US Department of the XXXX
Program Management Office

VERSION: 1.2
DATE: February 17, 2006

Documentation compiled by:

Joseph P. Holbrook, CHPTP, BCSD, BCFP, EMCPP
GOV CONTRACTOR GOV PROGRAM TEAM
GOV Location, GOV LOCATION STATE 22182

TABLE OF CONTENTS

Section Page

1.0 INTRODUCTION TO GOV PROGRAM

GOV PROGRAM (GOV PROGRAM), the combined effort of US Department of the Army(DLA) and other related logistics agencys agreed to establish several programs to update logistics programs. One of the programs related directly to the GOV PROGRAM project to replGOV PROGRAM the legacy Joint XXXXX (JTCOLLABORATION) program.

1.1 GOV PROGRAM GOV PROGRAM Capability

Smaller defense budgets and the changing threat hCollaboratione plGOV PROGRAM d the Department of Defense (DoD) under increased pressure to streamline its logistics process. Numerous "come-as-you-are" real-world situations hCollaboratione spotlighted the need to maintain a high state of readiness, and hCollaboratione starkly illustrated the imperative for providing visibility of the status and location of all assets throughout the DoD.

Significant changes in the archectecture of the COLLABORATION program will be implemented. JTCOLLABORATION GOV Location States a legacy based SUN unix server with direct attached storage which were located at the GOV Location Stater-fighting Commander in Charge (CINCS). The following CINCS or units had a JTCOLLABORATION server. JIFCOM, CENTCOM, EUCOMM, PACOM, KOREA & FT Belvioe

The new solution will be based on a centralized archectecture which will hCollaboratione the COLLABORATION components located at GOV PROGRAM in GOV PROGRAM, GOV LOCATION STATE and GOV Location, GOV LOCATION STATE. The future COLLABORATION solution, comprised in the GOV PROGRAM program will be based on a Hewlett Packard (HP) server solution with a StorageTek (HDS) SAN based disk storage.

The ability of a commander to "see" materiel across the logistics continuum (in-storage, in-process, and in-transit) has been the dream of GOV Location Stater-fighters and their logisticians from the inception of armed conflict. Recent developments in high-speed communications and logistics automation tools make it possible to provGOV PROGRAM (GOV PROGRAM) GOV PROGRAM capability for the Joint Task Force (JTF) Commander and GOV Location Stater-fighting CINCS.

The GOV PROGRAM GOV PROGRAM capability has been developed and implemented incrementally through continuous coordination with those organizations responsible for planning procedures and systems. Rather than a development effort, GOV PROGRAM GOV PROGRAM is an integration of capabilities. The GOV PROGRAM GOV PROGRAM capability is recognized as key to enabling and empowering the JTF Commanders, who hCollaboratione become pivotal players in executing national policy, to manage their materiel and personnel resources. GOV PROGRAM GOV PROGRAM represents a new capability to find and track personnel (both units and individuals), unit moves (materiel and equipment), and sustainment materiel from point-of-origin through arriGOV Location Statel at destination.

GOV PROGRAM GOV PROGRAM enables the display of data from disparate databases for users at the levels of GOV PROGRAM , JTF, Service component, and data element. GOV PROGRAM GOV PROGRAM has access to selected personnel data, all on-hand levels of supply, including ammunition, end-items, medical and repair parts, and materiel in-transit to the theater. Through a process unobserved by the user, GOV PROGRAM GOV PROGRAM Logistics maps and merges information from in-process, in-storage, and in-transit systems (or a combination of systems) to answer the JTF logistics questions. GOV PROGRAM GOV PROGRAM performs the interrogation process and displays the results in a GOV Location Stateriety of user-friendly formats.

1.2 Scope

The GOV PROGRAM System Administrator's Manual is intended to be a guide for the Database Administrator (DBA) and Systems Administrator (SA) at GOV PROGRAM sites in GOV Location, GOV LOCATION STATE, GOV PROGRAM, GOV LOCATION STATE and the current Reston Development site. This manual, which provides standardized procedures, implementing instructions, and general guidance, is intended to provide specific standard operating procedures for the GOV PROGRAM sites in GOV Location, GOV LOCATION STATE and GOV PROGRAM, GOV LOCATION STATE.

This manual also provides the basis to assist in the cross training the SA and DBA will need to deal with problems that could arise. It is imperative that all SAs and DBAs read and understand the material in the manual.

1.3 GOV PROGRAM GOV PROGRAM Architecture

GOV PROGRAM architecture is specifically designed with flexibility and commercial off-the-shelf (COTS) standardization. This architecture will easily assimilate and adapt to new applications and functions. This will also use high Collaborationailablility (HA) cluster capability to ensure continued GOV Location Stater-fighting capability.

The GOV PROGRAM GOV PROGRAM architecture is designed to be a flexible tool in the hands of the logistics planner. With continuing, effective SA/DBA activity, GOV PROGRAM GOV PROGRAM can achieve the end-state architecture involving complex systems design. Trained SA/DBA personnel are therefore essential to the satisfactory operation of the GOV PROGRAM GOV PROGRAM capability and to the resources at each GOV PROGRAM Server. This System Administrator's Manual provGOV PROGRAM s technical administration guidance for DoD sites utilizing GOV PROGRAM Asset Visibility

By means of an integrated logistics and personnel database, GOV PROGRAM GOV PROGRAM helps joint logistics planners meet their deliberate and crisis-data visibility tracking responsibilities. The objective of GOV PROGRAM COLLABORATION is not to create additional infrastructure, but to use the existing equipment and communications already in plGOV PROGRAM at the GOV PROGRAM level. To meet this goal, the GOV PROGRAM GOV PROGRAM database server is connected to a host Local Area Network/WGOV PROGRAM Area Network (LAN/GOV LOCATION STATEN) and the NIPRNET/SECURE NETWORK. This interconnects the GOV PROGRAM GOV PROGRAM server with a GOV Location Stateriety of workstations that run GOV PROGRAM .

DIAGRAM REMOVED CONFIDENTIAL

2.0 SYSTEM LEVEL DESCRIPTION OF GOV PROGRAM

At the center of the GOV PROGRAM capability are two primary functions: communications and data population. The following discussion is necessary to aid in the complete understanding of administrator functions.

2.1 GOV PROGRAM Communications

The GOV PROGRAM capability consists of a server with Oracle 9i RAC Database and web server softGOV Location Statere. The SECURE NETWORK server is updated via a one-GOV Location Statey feed from the NIPRNET server suite. An Imagery Support Server Environment (SECURE FTP APPLIANCE) Guard assures a single direction of data flow.

2.2 GOV PROGRAM Database

The GOV PROGRAM capability capitalizes on the asset visibility properties of existing logistics systems. The GOV PROGRAM capability integrates these capabilities into a single, transportable, user-friendly operational capability. GOV PROGRAM provs the /JTF Commander the capability to view assets , receive timely information on incoming assets, and initiate detailed logistics queries and analyses that used to be difficult to perform at the /JTF level.

The GOV PROGRAM Data contains General Supply Assets data, including packagedXXXXXXXX The queries for Inventory Status, Transportation, Requisition Status, GOV Location Stater Reserves, Unit Equipment, Bulk Fuel, Munitions, Medical, Utilities, and Reports can be executed. Additional functional and commodity areas being consred for future GOV PROGRAM releases include Maintenance and Personnel data. The GOV PROGRAM Database contains data from the Army, NCollaborationy, Air Force, Marine Corps, U.S. Transportation Command, and US Department of the Army(DLA) systems.

##DETERMINE STRUCTURE OF APP
The GOV PROGRAM application consists of the following segments:

DB — database segment
DR — reference segment (nomenclature tables)
DT — data transfer segment (repository for all incoming datafeeds)
WB — Web application segment
S — communications segment

###INSERT DATA SOURCES VISIO HERE###

Figure 2–1 Data Sources

3.0 HPUX ACCOUNT ADMINISTRATION FOR

3.1 Instructions on Creating an Unix Account

- Log-in as root, go into SAM.

- To start the administrator utility, from the command line type “sam &” > Users & Groups > Users

USER NTY

User Name - 8 letters for login purposes.
User ID - sequential number

300 - 399 Users (CONTRACTORS, GOV CONTRACTOR/PRIME CONTRACTOR & GOV Developers)
400 - 499 Datafeeds

Primary Group - Group Number from the following:
13 - Datafeeds
16 - Users
17 - dba (dba must hCollaboratione group to run certain commands in Oracle 9i Database and RAC)

Secondary Group - add secondary groups if necessary
Comment - User’s full name and pertinent information as necessary
Login Shell - Use kshell

ACCOUNT SECURITY

Password - Choose normal password and give a password to the user.
Min Change - 1 day
Max Change - follow local security directives
Max Inactive - follow local security directives
Expiration Date - follow local security directives
GOV Location Staterning - follow local security directives

HOME DIRECTORY(DETERMINE)

Create Home Directory - ensure button is depressed.
Path - all users directories will be under /usr/Collaboration.

3.2 Instructions for Deleting an Account

4.0 ORACLE 9I Real Application Clusters (RAC) RELATIONAL DATABASE MANAGEMENT SYSTEM OVERVIEW

The GOV PROGRAM Database is based on the ORACLE 9I RAC Relational Database Management System (RDBMS). This section provs a general overview of the ORACLE 9I RAC RDBMS. For specific information and operational instructions for ORACLE 9I RAC user access, backup/recovery procedures, ORACLE 9I RAC Database Administrator (DBA) utilities, and SQL*Plus, refer to the current version of the *ORACLE 9I RDBMS Database Administrator's Gu.* This document only describes the GOV PROGRAM Database and GOV PROGRAM Database Architecture. It presents detailed instructions for structural updates, message updates, and the GOV PROGRAM table structure.

The current versions of the following products are required for the implementation of highly Collaborationailable Oracle Real Application Clusters.The installation order of these softGOV Location Statere components are important for proper installation.

PRODUCT	VERSION	INSTALLATION ORDER
HPUX Operating System	11.11 Mission Critical OE	1
HPUX Patch Bundles	June 2004	2
Oracle	9.x.x.x	3
Oracle RAC	8.1.x.x	4
MC/ServiceGuard	At Shipping	5
ServiceGuard Extension for RAC	At SHipping	6

The current Oracle 9.1 RAC database version at the time of writing is 8.x.x. Oracle RAC relies on MC/ServiceGuard for its clustering capabilities.

####INSERT RAC VISIO

4.1 Database User Access and Privileges

Privileges prov control and management of access to a database. Before privileges can be granted to a user, an ORACLE 9I RAC user account must hCollaboratione been created. A user may also need a UNIX account (See Section 3 on creating a UNIX account), a Web account (See Section 12), or both, depending on how the database will be accessed.

To create an ORACLE 9I RAC user account, start an SQL*Plus session using a GOV Location Statelid DBA user-ID and password. Use the “CREATE USER …” statement to create the user account. Then grant the user appropriate privileges and/or roles (as a minimum, every user needs the CONNECT role). An example follows:

```
        create user jholbrook ntified by holbrook69
```

```
default tablesp USERS
temporary tablesp TEMP
quota unlimited on TEMP;

grant connect to jholbrook;
```

4.1.1 ORACLE 9I RAC Passwords

Each ORACLE 9I RAC database user account requires both user-name and password. User accounts are usually created by the DBA. As required, the DBA can change the password and grant or revoke specific privileges for any system user. Users can also change their own passwords. To change the password for a specific user, either the DBA or the user himself types the following:

```
alter user <username> ntified by <new_password>;
```

where <username> is the user's account name, and <new_password> is the changed password.

Privileges can be granted in two different GOV Location Stateys:

4.1.2 Explicit (Direct)

Direct User Access. Privileges can be granted to a user explicitly (directly). For example, a privilege to delete a record from table X_TEST in the database can be granted explicitly (directly) to the user "jholbrook". Example:

```
grant delete on X_TEST to jholbrook;
```

4.1.3 Roles

A role is a collection of data access privileges, and/or system privileges which can be granted to and revoked from multiple users simultaneously. Privileges can be granted to roles, and each role can be granted to one or more users. For example, a privilege to insert a record in the table COMMAND_CODES can be granted to the role _RO; this role can in turn be granted to the users "jholbrook" and "srenalds". A privilege to execute a particular application can be granted one or more roles and these roles can then be granted to the appropriate users.

```
grant insert, select on COMMAND_CODES to _ro;
grant execute on DB_LATEST_STATUS1 to _ro;

grant _ro to jholbrook, srenalds;
```

Roles can be provd by the DBA for individuals and groups of users for ease of use and management control. Privilege can be managed by reduction, dynamic assignment, selective Collaborationailability (enable or disable), application aGOV Location Statereness, and application-specific security.

A role can also be granted to other roles, which in turn can be granted to one or more users. Roles can be enabled or disabled at the user level.

a) The CONNECT role allows a user to create or alter a session (i.e., connect to a database), create a database link, create tables, views, synonyms, clusters, or sequences. When a session is created, a user can select information from tables or views he/she has created, or to which he/she has been given access by the table/view owner.

b) The RESOURCE role allows a user to create tables, clusters, sequences, triggers and procedures. The resource role also gives a user UNLIMITED TABLESP system privileges expicitly, not as part of the resource role. With the resource role, a user can grant or revoke access to schema objects in his/her own schema to and from other users. A user with the resource role must also hCollaboratione the connect role in order to connect to the database.

c) The DBA role allows users to perform the following actions:

- Access any user's data and perform any SQL statement upon it,
- Grant and revoke database system privileges, including WITH ADMIN OPTION,
- Create users, roles, public synonyms, and public database links,
- Control system-w auditing and table-level auditing defaults,
- Perform full database exports and imports, and
- Perform database-w maintenance operations such as adding tablesps and data files, setting tablesp on- or off-line, backing up tablesps, and archiving log files.

d) The EXP_FULL_ DATABASE role allows users to select any table, back up any table and insert, delete, and update certain system tables.

e) The IMP_FULL_DATABASE role allows users to log on as other users (i.e., BECOME USER) when performing full database imports.

The highest level of privileges and access to a database is limited to the DBA. To access a database, ordinary users must hCollaboratione a GOV Location Statelid ORACLE 9I RAC user-name and password, “CONNECT” role (a collection of privileges), and any other specific privileges or roles deemed necessary by the DBA (such as “RESOURCE”).

4.2 ORACLE 9I RAC Database Startup and Shut Down

The ORACLE 9I RAC database is not alGOV Location Stateys Collaborationailable to all users. To ensure control over the current status of the ORACLE 9I RAC database, only a DBA account can start up or shut down the ORACLE 9I RAC database. When a database is open, users can access the information in it. When a database is closed, users cannot access the information. This is desirable, at times, to prevent users from corrupting the database while diagnostic and maintenance procedures are being carried out.

4.2.1 Database Startup

Follow these steps to startup a database:

a. Log onto the database server as an Oracle 9i RAC DBA.

b. At the UNIX prompt, type “**dbstart”**.

4.2.2 Database Shutdown

An ORACLE 9I RAC database can be shut down using one of three options:

- SHUTDOWN NORMAL (the default): ORACLE 9I RAC GOV Location Stateits for currently enrolled users to disconnect from the database, prohibits new users from logging in, closes and dismounts the database, and shuts down the instance. Shutdown normal is accomplished via the **dbshut** command at the UNIX prompt (see Paragraph 5.5.3).

- SHUTDOWN IMMEDIATE: ORACLE 9I RAC immediately terminates any current client SQL statement being processed (it does not GOV Location Stateit for users currently connected to the database to disconnect) and rolls back the uncommitted statements. This option should be used when a reboot or power shutdown is anticipated, or when the database is functioning irregularly. Shutdown immediate is accomplished by entering “shutdown immediate” instead of “shutdown” or “shutdown normal” (see Paragraph 5.5.3). Under normal GOV PROGRAM circumstances, the shutdown immediate option is recommended.

- SHUTDOWN ABORT: ORACLE 9I RAC immediately terminates any current client SQL statement being processed (without GOV Location Stateiting for users to disconnect), uncommitted transactions are not rolled back, and the database instance is immediately aborted. The next startup of the database will require instance recovery procedures (automatically performed during database startup). This option should be used only when both normal and immediate shutdown procedures fail, or when there is difficulty starting a database instance. Shutdown abort is accomplished by entering, “shutdown abort” instead of “shutdown,” “shutdown normal,” or “shutdown immediate” (see Paragraph 5.5.3).

The following steps are required to shutdown an open database:

a. Log on to the database server and enter “su - <dba>” to log in as an ORACLE 9I RAC DBA (where <dba> is a GOV Location Statelid UNIX account for a member of the DBA Group and has been granted the ORACLE 9I RAC DBA role).

b. To shutdown the database normally (see description above), at the UNIX prompt type “**dbshut**” (without the quotes), or alternatively,

4.3 Net 8

Net 8 is ORACLE 9I RAC’s remote data access softGOV Location Statere and enables client/server communications across the networks.

An applicable listener to field the requests and forGOV Location Staterd them to the specified database must exist to communicate with the ORACLE 9I RAC database. GOV PROGRAM uses the Net 8 listener, tnslsnr. The listener runs on the database server. The primary network protocol is TCP/IP, but some communications use the IPC protocol.

To determine whether the Net 8 listener is running on the database server, logon to the server using a GOV Location Statelid UNIX DBA account (i.e., an account which is a member of the DBA group). At the UNIX prompt, enter:

```
lsnrctl stat
```

Alternatively, at the UNIX prompt, enter:

```
ps -ef | grep tnslsnr
```

(*tnslsnr* is the name of the Net 8 listener on the database server).

To start the Net 8 listener, at the UNIX prompt, enter:

```
      lsnrctl start
```

To stop the Net 8 listener, at the UNIX prompt, enter:

```
      lsnrctl stop
```

There are three ASCII files associated with the Net 8 softGOV Location Statere:

- listener.ora,
- tnsnames.ora, and
- sqlnet.ora.

The default directory where the files *listener.ora*, *sqlnet.ora* and *tnsnames.ora*

.####(INSERT HOME LOCATION)

If it becomes necessary to edit these files, a UNIX editor such as **vi** can be used. Users must be careful not to inadvertently add or delete any "extra characters" in these files, in particular, trailing parentheses.

The *listener.ora* file defines the local server to Net 8. An example of a *listener.ora* file follows:

```
######INSERT LISTENER.ORA FILE
```

The *tnsnames.ora* file which ress on each database server contains connect strings and descriptions of databases on other servers. A connect description is a specially formatted description of the destination for a network connection, consisting of sets of keywords and GOV Location Statelues. It lists the communities of which the client is a member, the community protocol, i.e., TCP/IP, host name (or alternately, IP address) and the UNIX Port number allocated. If connection data changes, then each copy of the *tnsnames.ora* file on all GOV PROGRAM   servers should be updated.

########INSERT TNSNAMES.ORA FILE

The connect strings in the GOV PROGRAM   *tnsnames.ora* typically take the form of *<hostname>.world.* Some examples of GOV Location Statelid Net 8 connection strings are:

- dlaas11.world
- dladb02.world

The connect description for a given connect string contains much of the same information as the *listener.ora* file for server being described. A partial example of a *tnsnames.ora* file follows:

```
##### INSERT SQL*Net Configuration file ####
```

4.4 Full Database Export

To export the entire database, either for backup or to populate another machine, the DBA can create a full database export using ORACLE 9I RAC's export utility 'exp'. This will export all objects, procedures, grants, synonyms, etc., owned by the user specified (typically 'dba'), along with all the "generic" ORACLE 9I RAC system objects and procedures stored in the SYSTEM tablesp.

The database is quite small (barely over 15 Gbytes), so the export file for a full database export created by the export utility will be large as well (typically 5–8 Gbytes). You will need a hard disk location with sufficient sp to create this large file to perform a full database export.

To export the full database, **change directory** to the new export directory that has sufficient sp as described above, then enter the command "su - <oradba>" (where <oradba> is a GOV Location Statelid UNIX account which is a member of the DBA group). Then enter the command:

```
exp <dba-id>/<dba-pw> parfile=<path>/exp_full.par
```

where <dba-id>/<dba-pw> is the ORACLE 9I RAC user-id and password for the database owner account (typically dba), and <path> is the UNIX path to the location of the exp_full.par export parameter file described below.

```
FILE=full_exp.dmp
COMPRESS=N
FULL=Y
LOG=full_exp.log
```

4.5 Correcting Database Fragmentation

A message pile-up occurs when the maximum number of extents for a table is exceeded. The following procedure provs a solution to this problem:

- Log-in using a GOV Location Statelid UNIX user-id in the DBA group (or enter "su - <oradba>" where <oradba> us a GOV Location Statelid UNIX user-id in the DBA group).

- Export table using ORACLE 9I RAC export command. Enter "exp <dba-id>/<dba-pw>" at the UNIX prompt (where <dba-id>/<dba-pw> is the ORACLE 9I RAC owner id and password for the database – typically "dba"), and then answer the following questions appropriately. The default answer to each question is given after the colon; if the default GOV Location Statelue is acceptable, simply enter <RETURN>; otherwise, enter the GOV Location Statelue you GOV Location Statent. To fix the fragmentation of a table, make sure you say "yes" to compress extents. An example follows:

```
Enter array fetch buffer size:  4096 >  2097152<RETURN>

Export file:  expdat.dmp >  reqn.dmp

(1)E(ntire database), (2)U(sers), or (3)T(ables):  (2)U >  T

Export table data (yes/no):  yes >  <RETURN>

Compress extents (yes/no):  yes >  no<RETURN>
```

```
Export done in US7ASCII character set

About to export specified tables via Conventional Path ...
Table to be exported:  (RETURN to quit) >  REQUISITION

. . exporting table      REQUISITION        1170644 rows
exported
Table to be exported:  (RETURN to quit) >  <RETURN>

Export terminated successfully without GOV Location Staternings.
```

- Drop the releGOV Location Statent table using SQL*Plus,

  ```
  SQL>  drop table requisition cascade constraints;

  Table dropped.
  ```

- Import the sCollaborationed table by using the ORACLE 9I RAC import command. At the UNIX prompt, enter “imp <dba-id>/<dba-pw>” (where <dba-id>/<dba-pw> is the ORACLE 9I RAC user-id and password for the database owner – typically “dba”). Respond to the program queries appropriately. The default answer to each question is given after the colon; if the default GOV Location Statelue is acceptable, simply enter <RETURN>, otherwise enter the GOV Location Statelue you desire. Ensure that the answer to “import grants?” is yes.

This procedure must be accomplished without any user or process accessing the releGOV Location Statent table.

4.6 Determining Free Sp in a Tablesp

Start SQL*Plus as the database owner account (typically dba). At the SQL> prompt, type the following statement:

```
SQL>  select sum(bytes) from user_free_sp
  2> where tablesp_name = '<tablesp>';
```

where <tablesp> is the name of the tablesp in question, entered in all upper-case.

4.7 Oracle DB Monitoring

The ORACLE 9I RAC routines described here are used to monitor the state of the database. They can help Collaborationoid problems and aid in troubleshooting errors. The reports generated by these routines indicate when a tablesp is full or approaching full. When a tablesp is full, adding another data file can often correct these problems.

These utilities are very useful when a tablesp becomes too full or when a database object attempts to exceed its MAX _EXTENTS. The database can be monitored daily and status reports can be produced. This process enables the DBA to spot and eliminate many potential problems before they occur. Also, the routines enable the DBA to regulate and schedule some of the database “repair work”.

These routines can be run daily by placing them in the DBA's "crontab" file. When this is done, the routines will access the database at the designated time and will create an output file containing useful information about database storage sp. The script file can concatenate the information files and E-mail them to the interested parties. The programs were designed to be run weekly, but they can easily be run daily. It requires one month to accumulate a usable amount of data in the CHANGED column of the reports.

Shell Scripts

##INSERT HERE

4.8 GOV PROGRAM COE (Common Operating Environment)

- XXXX: The main database segment contains all scripts and files needed for GOV PROGRAM database installation, maintenance, source files for stored procedures, load-scripts and data-stores (*.dbf files).
- XXXX: The data segment is the staging area for feeds to the GOV PROGRAM capability.
- XXXX: The Web server segment.

4.8.1 Directory Structure of Database

#####INSERT DIRECTORY STRUCTURE

4.8.2 GOV PROGRAM Users

The UNIX group-id is defined during DB installation. This group consists of one user, 'dba'. The purpose of this group is to limit '.orapwd' file access to only 'dba'. The '. orapwd' contains the ORACLE 9I RAC password of 'dba' and 'jlog_ftp'. The GOV PROGRAM group is only a temporary solution to protect password information. It will not be needed once COE provs us with a password-handling tool.

4.8.2.1 UNIX Users

####INSERT GLOBAL PROFILE HERE

4.8.2.2 ORACLE 9I RAC Users:

4.9 Application Profiles

Oracle Profiles:

######INSERT ORACLE PROFILE HERE

Web Profiles

#####INSERT WEB PROFILES

5.0 DATAFEED SECTION

REMOVED !! CONFIDENTIAL

6.0 GOVERNMENT PROPERTY OVERVIEW

6.1 Property Accountability

All Government property, either contractor-acquired or Government-furnished equipment (GFE), regardless of location, must be accounted for as required by Federal Acquisition Regulations (FAR). GOV CONTRACTOR/PRIME CONTRACTOR (GOV CONTRACTOR/PRIME CONTRACTOR) will maintain approved property control procedures and current, detailed records of all Government property in GOV CONTRACTOR/PRIME CONTRACTOR's possession, whether provd directly by the

Government as Government-furnished property (GFP) or purchased by GOV CONTRACTOR/PRIME CONTRACTOR on behalf of the Government as contractor-acquired property (CAP). The Program Manager is responsible for property accountability, and will designate a Property Custodian who will serve as the primary point of contact at the Program level and coordinate with the Corporate Property Administrator (CPA) for all matters related to GOV CONTRACTOR/PRIME CONTRACTOR Property Administration on the contract. This is consistent with both contract and corporate requirements. The Program Manager will be consred the Property Custodian's alternate.

GOV CONTRACTOR/PRIME CONTRACTOR acquires CAP only when it is required for performance of the contract and contractually authorized in adGOV Location Statence. The cost of this property is charged directly to the contract. The Government has title to this property. GOV CONTRACTOR/PRIME CONTRACTOR-acquired Government property will be procured in accordance with the procedures set forth by GOV CONTRACTOR/PRIME CONTRACTOR's Government-approved purchasing system.

6.1.1 Inventory (GFE at RESTON)

A list of inventory will be kept current at all times and must include the following:

- Purchase Requisition (PR) Number
- Purchase Order (PO) Number
- Date received
- Item Description (manufacturer, make, and model)
- Serial Number
- Prime Contract Number and Project Number
- Cost/Estimated GOV Location Statelue
- Room Location
- Property Tag Number.

Each item of Government property will hCollaboratione a GOV CONTRACTOR/PRIME CONTRACTOR property tag and a Government property tag printed with the contract number. The GOV CONTRACTOR/PRIME CONTRACTOR property tag contains a serialized GOV CONTRACTOR/PRIME CONTRACTOR Designator Number and will be pld on the property by the GOV CONTRACTOR/PRIME CONTRACTOR central receiving facility or by the designated Property Custodian receiving the property. The Government property tag will be requested and pld on the equipment by the Property Custodian. If property is drop-shipped to a GOV CONTRACTOR/PRIME CONTRACTOR facility other than the central receiving facility, the Property Custodian will also complete a Receiving/Inspection Report and forGOV Location Staterd it to the Purchasing Department with a copy to the CPA.

When GOV CONTRACTOR/PRIME CONTRACTOR receives GFE, the Property Custodian will complete a form DD1149 acknowledging receipt. This form is forGOV Location Staterded to the CPA for inclusion in GOV CONTRACTOR/PRIME CONTRACTOR's property records. The Property Custodian will request the necessary property tags from the CPA and add these items to the inventory list.

6.1.2 Movement

Any movement of Government property, for any reason, to a different GOV CONTRACTOR/PRIME CONTRACTOR facility will be made only with the adGOV Location Statence approGOV Location Statel of the CPA. The Property Custodian will request this approGOV Location Statel.

6.1.3 Return of Government Property

When a contract ends or when the requirement to hCollaboratione the items in GOV CONTRACTOR/PRIME CONTRACTOR's possession no longer exists, GOV CONTRACTOR/PRIME CONTRACTOR will return the property to the Government. The return of Government property is documented on a standard form DD 1149 (see discussion below) and the items are removed from GOV CONTRACTOR/PRIME CONTRACTOR's inventory. The Property Custodian will remove all property tags before returning the equipment and forGOV Location Staterd them to the CPA.

6.1.4 Co-Mingling of Property

All Government property will be kept physically separate from GOV CONTRACTOR/PRIME CONTRACTOR-owned property. In no case should GOV CONTRACTOR/PRIME CONTRACTOR and Government property be co-mingled unless specifically approved.

6.1.5 Procedures for Using Form DD 1149

A standard form DD 1149 is completed when GOV CONTRACTOR/PRIME CONTRACTOR either receives or returns Government PROPERTY. The Property Custodian is responsible for completing this form. The DD 1149 form contains the item description, serial number and estimated GOV Location Statelue for each item. The Government employee receiving the property will sign for the items immediately upon receipt. After the Government has signed for the property, the original DD 1149 form is forGOV Location Staterded, along with the property tags, to the CPA who will remove the items from the official GOV CONTRACTOR/PRIME CONTRACTOR property records.

6.2 Maintenance

6.2.1 Scheduled Server Maintenance

Scheduled Maintenance includes system backups, daily administrative system cleanup, and periodic system shutdowns. Administrators at each site should develop their own plans to carry out system backups according to server usage.

6.2.3 Shutdown or Reboot

HPUX servers should be shut down and restarted every 30 Days. This will allow system buffers to clear and to reset the processes that run continuously. The command to shutdown the server is the following:

```
shutdown –h –y 0
```

where:

-h is the init state (init state 0 is HALT)
-y automatically answers all questions to prevent user prompts
-0 is the gr period (60 seconds is the default, 0 is immediate)

or

```
reboot
```

(System will come back up to default init state)

NOTE: If there are and background or hung Oracle 9i RAC processes running, the DBA will need to shutdown the database manually (using shutdown abort) prior to performing the system shutdown. Otherwise the server will GOV Location Stateit until all Oracle 9i RAC processes are completed prior to shutting down the system.

6.2.4 Daily Administrative Cleanup (HPUX and Oracle)

The SA will perform the following on a daily routine to check system operation, and cleanup.

SA's are to archive and maintain security logs in accordance with security directives.

Change directory (cd) to the following directories and perform functions as necessary.

/tmp

Remove any extraneous files from the directory. Extraneous files include:

lock* files
crout* files
tmp files

/GOV Location Stater/tmp

Remove any extraneous files from the directory.

These are files that start with Ex*, Rx*, stm* and wscon*.

/GOV Location Stater/adm

Edit the following files. Verify system operation. Verify normal operations of the server. Clean up files by deleting all lines, and sCollaborationing file.

syslog - file is ASCII. Check for server operations and logins.
sulog - file is ASCII. Check for people trying to break certain passwords.

The following files can be cleaned up when they are too large (over 50K):

utmp - file is encoded
utmpx - file is encoded.
wtmp - file is encoded.
wtmpx - file is encoded.

Performing "last > /security2/loginlog.MMDD" (MM=Month, DD=Day), will sCollaboratione the contents of the wtmp and wtmpx files for future reference. Then the System Administrator can clean out the wtmp and wtmpx logs on a daily basis and review the loginlog.MMDD file to check who has been on the system. These logs should be kept for six months before deleting.

Perform a vi on the file and use d *nn* to delete all the information in the file.

/GOV Location Stater/mail

Check to see who has mail. Ensure dba checks mail daily for crontab operations of loading data into database. Delete any mail that is more than 30 days old.

/GOV Location Stater/adm/syslog

Edit the syslog file. Check for failed login attempts. Report failed login attempts from unknown sources to the Security Officer. Clean up the file by deleting all text, and sCollaborationing the file.

/GOV Location Stater/cron

Edit the log file. Clean up the file by deleting all the text and sCollaborationing the file.

Prior to performing the following cleanup on the Oracle 9i RAC areas, ensure that the DBA has completed all checks on the loading of the database.

####VERIFY ORACLE LOGS

An alert log (*.log) file will be present. The DBA needs to review the clean up.
Tr files (*.trc) will be present. The DBA will need to review and clean up as necessary.

The DBA will need to review Audit files(if created) and clean up as necessary.

Edit the listener.log to verify the users coming in through sqlnet. Clean up file by deleting all the lines and sCollaborationing the file.

Edit the sqlnet.log file, delete the information and sCollaboratione the file. This file lists the startup of sqlnet.

Perform disk usage command (bdf) and check disk usage. Certain drives will be above 80% full, the database should be residing on those directories. If the root directory (/) or /h drives are full, the SA must clean out old files.

Perform a process status command (ps –ef) and check for any process that is hung, or has been running for an excessive amount of time. Especially GOV Location Statetch for hung ftp processes and long Oracle 9i RAC load or query processes. If there is a hung Oracle 9i RAC load process, inform the DBA so that the process can be checked. Kill any hung processes using the following kill command:

```
kill –9 <PROCESS_ID>
```

6.2.5 Weekly Cleanup

##SPECIFY

6.2.6 Monthly Cleanup

###SPECIFY

6.2.7 Backups

The system administrator will be responsible for performing system backups and maintaining backup tapes. Backups should not interfere with normal operation of . The Oracle 9i RAC database must be shut down so the synchronization of the database files remains intact. If a backup of the system is performed while the database is on-line, the database files will be useless for a frecover.

A FULL backup will be performed upon system acceptance at each site and then upon each major system upgrade. The only other time a FULL level backup needs be performed is after a major server upgrade. Otherwise, only areas that hCollaboratione changes will be backed up on a weekly basis.

Procedures for performing backups and restores are covered in Section 8.

6.2.8 Mirrored Boot Disk (Boot Mirror)

HP MirrorDisk/UX is used to create mirrors. The process can be accomplished using for non-boot disks such as /opt, /oracle etc. However, one of the weaknesses of SAM is that you can not create bootable mirrors. The following process must be utilized to accomplish this.

```
    MirrorDisk/UX is an optional product that is utilized for mirroring
Logical Volume Manager(LVM) disks on HPUX platforms. This product is
extremely easy to use and can be administered though command line and
```

SAM.(Note, SAM can not create a “bootable” mirror). We will document the command line process.

Below are the instructions to mirror the primary disk filesystems and sGOV Location Statep. In this configuration we only hCollaboratione two disks and one Volume Group. The primary disks will be mirrored to secondary disk in the Volume Group 00 (VG00)

EXTEND VOLUME GROUP

1. Determine the device file of the secondary disk. Ioscan is the perfect command for this.

```
# ioscan -fnC disk

Class     I  H/W Path       Driver  S/W State   H/W Type     Description

=========================================================================

disk      0  0/0/2/0.0.0.0  sdisk   CLAIMED     DEVICE       TEAC    DV-28E-C

                           /dev/dsk/c0t0d0   /dev/rdsk/c0t0d0

disk      1  0/1/1/0.0.0    sdisk   CLAIMED     DEVICE       HP
73.4GST373453LC

                           /dev/dsk/c2t0d0   /dev/rdsk/c2t0d0

disk      2  0/1/1/0.1.0    sdisk   CLAIMED     DEVICE       HP
73.4GST373453LC

                           /dev/dsk/c2t1d0   /dev/rdsk/c2t1d0
```

2. Verify vg00 configuration. You will notice that there is one Physical Volume (PV).

```
# vgdisplay -v vg00


--- Volume groups ---

VG Name                     /dev/vg00

VG Write Access             read/write

VG Status                   Collaborationailable

Max LV                      255

Cur LV                      8

Open LV                     8

Max PV                      16

Cur PV                      1

Act PV                      1

Max PE per PV               4384

VGDA                        2

PE Size (Mbytes)            16

Total PE                    4374
```

```
Alloc PE                    853

Free PE                     3521
Total PVG                   0
Total Spare PVs             0
Total Spare PVs in use      0


   --- Logical volumes ---
   LV Name                     /dev/vg00/lvol1
   LV Status                   Collaborationailable/syncd

Standard input
   LV Size (Mbytes)            304
   Current LE                  19
   Allocated PE                19
   Used PV                     1


   LV Name                     /dev/vg00/lvol2
   LV Status                   Collaborationailable/syncd
   LV Size (Mbytes)            4096
   Current LE                  256
   Allocated PE                256
   Used PV                     1


   LV Name                     /dev/vg00/lvol3
   LV Status                   Collaborationailable/syncd
   LV Size (Mbytes)            208
   Current LE                  13
   Allocated PE                13
   Used PV                     1


   LV Name                     /dev/vg00/lvol4
   LV Status                   Collaborationailable/syncd
   LV Size (Mbytes)            208
   Current LE                  13
Standard input
   Allocated PE                13
Standard input
   Used PV                     1


   LV Name                     /dev/vg00/lvol5
   LV Status                   Collaborationailable/syncd
   LV Size (Mbytes)            32
   Current LE                  2
   Allocated PE                2
   Used PV                     1


   LV Name                     /dev/vg00/lvol6
   LV Status                   Collaborationailable/syncd
   LV Size (Mbytes)            2192
   Current LE                  137
   Allocated PE                137
   Used PV                     1


   LV Name                     /dev/vg00/lvol7
   LV Status                   Collaborationailable/syncd
   LV Size (Mbytes)            2000
   Current LE                  125
   Allocated PE                125
   Used PV                     1


Standard input
   LV Name                     /dev/vg00/lvol8

Standard input
   LV Status                   Collaborationailable/syncd
   LV Size (Mbytes)            4608
   Current LE                  288
   Allocated PE                288
   Used PV                     1



   --- Physical volumes ---
   PV Name                     /dev/dsk/c2t0d0
   PV Status                   Collaborationailable
   Total PE                    4374
   Free PE                     3521
   Autoswitch                  On
```

3. Create a Physical Volume on the secondary disk /dev/dsk/c2t1d0.

```
# pvcreate -B /dev/rdsk/c2t1d0
Physical volume "/dev/rdsk/c2t1d0" has been successfully created.
```

4. Extend the volume group vg00 with the new physical volume.

```
# vgextend /dev/vg00 /dev/dsk/c2t1d0

Volume group "/dev/vg00" has been successfully extended.

Volume Group configuration for /dev/vg00 has been sCollaborationed in
/etc/lvmconf/vg00.conf
```

5. Pl boot utilities on disk

```
# mkboot /dev/rdsk/c2t1d0
```

6. Add the AUTO file to the boot LIF

```
# mkboot -a "hpux -lq /stand/vmunix" /dev/rdsk/c2t1d0
```

7. Review the Filesystem layout(specifically the lvols)

```
# bdf

Filesystem          kbytes    used   Collaborationail %used Mounted on

/dev/vg00/lvol3     212992   88416  123648   42% /

/dev/vg00/lvol1     298928   41384  227648   15% /stand

/dev/vg00/lvol8    4718592  402984 4282296    9% /GOV Location Stater

/dev/vg00/lvol7    2048000 1144704  896248   56% /usr

/dev/vg00/lvol4     212992    2464  208952    1% /tmp

/dev/vg00/lvol6    2244608 1611232  628440   72% /opt

/dev/vg00/lvol5      32768    2392   30152    7% /home

dccsofs04.agc.local:/vol/proj/sudo

                   915941648 823250224 92691424   90% /usr/local/sudo
```

8. Review the sGOV Location Statepinfo and verify lvol

```
# sGOV Location Statepinfo

             Kb      Kb      Kb   PCT  START/      Kb

TYPE      COLLABORATIONAIL    USED    FREE  USED   LIMIT RESERVE  PRI  NAME

dev     4194304       0 4194304    0%       0       -    1  /dev/vg00/lvol2

reserve       -  172720 -172720
memory  1568380  180988 1387392   12%
```

EXTEND LOGICAL VOLUMES

9. Extend the logical volumes. (lvols) You must run lvextend for each logical volume. There are eight total.

```
# lvextend -m 1 /dev/vg00/lvol1 /dev/dsk/c2t1d0

The newly allocated mirrors are now being synchronized. This operation will

take some time. Please GOV Location Stateit ....

Logical volume "/dev/vg00/lvol1" has been successfully extended.

Volume Group configuration for /dev/vg00 has been sCollaborationed in
/etc/lvmconf/vg00.conf


# lvextend -m 1 /dev/vg00/lvol2 /dev/dsk/c2t1d0

The newly allocated mirrors are now being synchronized. This operation will

take some time. Please GOV Location Stateit ....

Logical volume "/dev/vg00/lvol2" has been successfully extended.

Volume Group configuration for /dev/vg00 has been sCollaborationed in
/etc/lvmconf/vg00.conf



# lvextend -m 1 /dev/vg00/lvol3 /dev/dsk/c2t1d0

The newly allocated mirrors are now being synchronized. This operation will

take some time. Please GOV Location Stateit ....

Logical volume "/dev/vg00/lvol3" has been successfully extended.

Volume Group configuration for /dev/vg00 has been sCollaborationed in
/etc/lvmconf/vg00.conf


# lvextend -m 1 /dev/vg00/lvol4 /dev/dsk/c2t1d0

The newly allocated mirrors are now being synchronized. This operation will

take some time. Please GOV Location Stateit ....

Logical volume "/dev/vg00/lvol4" has been successfully extended.

Volume Group configuration for /dev/vg00 has been sCollaborationed in
/etc/lvmconf/vg00.conf


# lvextend -m 1 /dev/vg00/lvol5 /dev/dsk/c2t1d0
```

```
The newly allocated mirrors are now being synchronized. This operation will

take some time. Please GOV Location Stateit ....

Logical volume "/dev/vg00/lvol5" has been successfully extended.

Volume Group configuration for /dev/vg00 has been sCollaborationed in
/etc/lvmconf/vg00.conf


# lvextend -m 1 /dev/vg00/lvol6 /dev/dsk/c2t1d0

The newly allocated mirrors are now being synchronized. This operation will

take some time. Please GOV Location Stateit ....

Logical volume "/dev/vg00/lvol6" has been successfully extended.

Volume Group configuration for /dev/vg00 has been sCollaborationed in
/etc/lvmconf/vg00.conf


# lvextend -m 1 /dev/vg00/lvol7 /dev/dsk/c2t1d0

The newly allocated mirrors are now being synchronized. This operation will

take some time. Please GOV Location Stateit ....

Logical volume "/dev/vg00/lvol7" has been successfully extended.

Volume Group configuration for /dev/vg00 has been sCollaborationed in
/etc/lvmconf/vg00.conf


# lvextend -m 1 /dev/vg00/lvol8 /dev/dsk/c2t1d0

The newly allocated mirrors are now being synchronized. This operation will

take some time. Please GOV Location Stateit ....

Logical volume "/dev/vg00/lvol8" has been successfully extended.

Volume Group configuration for /dev/vg00 has been sCollaborationed in
/etc/lvmconf/vg00.conf
```

VERIFY CONFIGURATION

10. Verify the boot information.

```
#lvlnboot -v
Boot Definitions for Volume Group /dev/vg00:

Physical Volumes belonging in Root Volume Group:

        /dev/dsk/c2t0d0 (0/1/1/0.0.0) -- Boot Disk

        /dev/dsk/c2t1d0 (0/1/1/0.1.0) -- Boot Disk

Boot: lvol1     on:     /dev/dsk/c2t0d0

                        /dev/dsk/c2t1d0

Root: lvol3     on:     /dev/dsk/c2t0d0

                        /dev/dsk/c2t1d0

SGOV Location Statep: lvol2     on:     /dev/dsk/c2t0d0

                        /dev/dsk/c2t1d0

Dump: lvol2     on:     /dev/dsk/c2t0d0, 0
```

11. Verify the updated vg00 physical volumes.

```
# vgdisplay -v vg00

--- Volume groups ---

VG Name                     /dev/vg00

VG Write Access             read/write

VG Status                   Collaborationailable

Max LV                      255

Cur LV                      8

Open LV                     8

Max PV                      16

Cur PV                      2

Act PV                      2

Max PE per PV               4384

VGDA                        4
```

```
PE Size (Mbytes)            16
Total PE                    8748
Alloc PE                    1706
Free PE                     7042
Total PVG                   0
Total Spare PVs             0
Total Spare PVs in use      0

   --- Logical volumes ---
   LV Name                     /dev/vg00/lvol1
   LV Status                   Collaborationailable/syncd
   LV Size (Mbytes)            304
   Current LE                  19
   Allocated PE                38
   Used PV                     2

   LV Name                     /dev/vg00/lvol2
   LV Status                   Collaborationailable/syncd
   LV Size (Mbytes)            4096
   Current LE                  256
   Allocated PE                512
   Used PV                     2

   LV Name                     /dev/vg00/lvol3
   LV Status                   Collaborationailable/syncd
   LV Size (Mbytes)            208
   Current LE                  13
   Allocated PE                26
```

```
Used PV                     2

LV Name                     /dev/vg00/lvol4
LV Status                   Collaborationailable/syncd
LV Size (Mbytes)            208
Current LE                  13
Allocated PE                26
Used PV                     2

LV Name                     /dev/vg00/lvol5
LV Status                   Collaborationailable/syncd
LV Size (Mbytes)            32
Current LE                  2
Allocated PE                4
Used PV                     2

LV Name                     /dev/vg00/lvol6
LV Status                   Collaborationailable/syncd
LV Size (Mbytes)            2192
Current LE                  137
Allocated PE                274
Used PV                     2

LV Name                     /dev/vg00/lvol7
LV Status                   Collaborationailable/syncd
LV Size (Mbytes)            2000
Current LE                  125
Allocated PE                250
```

```
Used PV                      2

LV Name                      /dev/vg00/lvol8
LV Status                    Collaborationailable/syncd
LV Size (Mbytes)             4608
Current LE                   288
Allocated PE                 576
Used PV                      2



--- Physical volumes ---
PV Name                      /dev/dsk/c2t0d0
PV Status                    Collaborationailable
Total PE                     4374
Free PE                      3521
Autoswitch                   On

PV Name                      /dev/dsk/c2t1d0
PV Status                    Collaborationailable
Total PE                     4374
Free PE                      3521
Autoswitch                   On
```

TEST THE MIRROR

To test the mirror we need to reboot and boot of the newly created mirror.

12. Enter "reboot" . System will reboot and allow you to interrupt the boot process.

13. Ensure you are on a system console. Enter login info.

```
MP password: *****


MP login: Admin
MP password: *****




                     Hewlett-Packard Management Processor

    (c) Copyright Hewlett-Packard Company 1999-2003.  All Rights Reserved.

                           MP Host Name: uninitialized

                              Revision E.02.26


*************************************************************************
                        MP ACCESS IS NOT SECURE
 Default MP users are currently configured and remote access is enabled.
 Modify default users passwords or delete default users (see UC command)
                                   OR
           Disable all types of remote access (see SA command)
*************************************************************************


   MP MAIN MENU:

         CO: Console
        VFP: Virtual Front Panel
         CM: Command Menu
         CL: Console Log
         SL: Show Event Logs
        CSP: Connect to Service Processor
         SE: Enter OS Session
         HE: Main Help Menu
          X: Exit Connection

[uninitialized] MP> co



        (Use Ctrl-B to return to MP main menu.)
```

```
- - - - - - - - - - - Prior Console Output - - - - - - - - - -
Closing open logical volumes...
Done



FirmGOV Location Statere Version  44.6

Duplex Console IO Dependent Code (IODC) revision 1



- - - - - - - - - - - - - Live Console - - - - - - - - - - - -
```

14. Now you must stop boot process by selecting any key. Follow the RED commands and enter at the appropriate prompts.

```
FirmGOV Location Statere Version  44.6

Duplex Console IO Dependent Code (IODC) revision 1
-----------------------------------------------------------------------------
-
   (c) Copyright 1995-2004, Hewlett-Packard Company, All rights reserved
-----------------------------------------------------------------------------
-

  Processor   Speed            State            CoProcessor State  Cache Size
  Number                                        State              Inst
Data
  ---------  --------   ---------------------   -----------------  -----------
-
      0      800  MHz   Active                  Functional         33554432
33552
      1      800  MHz   Idle                    Functional         33554432
33552

  Central Bus Speed (in MHz)  :        200
  Collaborationailable Memory            :    2097152  KB
  Good Memory Required        : Not initialized. Defaults to 32 MB.

   Primary boot path:    0/1/1/0.0
   Alternate boot path:  0/0/2/0.3
   Console path:         0/7/1/1.0
   Keyboard path:        0/0/4/0.0


Processor is booting from the first Collaborationailable device.

To discontinue, press any key within 10 seconds.

Boot terminated.
```

15. At the following "Main Menu" :Enter command or menu: interf below we must specify the boot device. We can find Collaborationailable boot devices by entering the "SEA" command. You can also use the "CO" command to view current boot GOV Location Statelues set in memory.

```
---- Main Menu --------------------------------------------------------------
-

     Command                          Description
     -------                          -----------
     BOot [PRI|ALT|<path>]            Boot from specified path
     PAth [PRI|ALT] [<path>]          Display or modify a path
     SEArch [DIsplay|IPL] [<path>]    Search for boot devices

     COnfiguration menu               Displays or sets boot GOV Location
Statelues
     INformation menu                 Displays hardGOV Location Statere
information
     SERvice menu                     Displays service commands

     DIsplay                          Redisplay the current menu
     HElp [<menu>|<command>]          Display help for menu or command
     RESET                            Restart the system
----

Main Menu: Enter command or menu > sea

Searching for potential boot device(s)
This may take several minutes.

To discontinue search, press any key (termination may not be immediate).



IODC
   Path#  Device Path (dec)  Device Path (mnem)  Device Type
Rev
   -----  -----------------  ------------------  -----------               --
--
   P0     0/0/2/0.0          .0                 Random access media       0
   P1     0/1/1/0.1          intscsia.1            Random access media       0
   P2     0/1/1/0.0          intscsia.0            Random access media       0
   P3     0/3/1/0.0                                Random access media       6
   P4     0/4/1/0.0                                Random access media       6


Main Menu: Enter command or menu > bo p2

Interact with IPL (Y, N, or Cancel)?> y
Booting...
Boot IO Dependent Code (IODC) revision 0


HARD Booted.

ISL Revision A.00.43  Apr 12, 2000

ISL>
```

16. Now at the ISL> prompt enter the command to boot."hpux"

```
ISL> hpux
```

```
Boot
: disk(0/1/1/0.0.0.0.0.0.0.0;0)/stand/vmunix
10964992 + 2052096 + 1419600 start 0x1f77e8



alloc_pdc_pages: Relocating PDC from 0xffffff0f0c00000 to 0x3f900000.
```

17. System will continue its boot process. At the completion of the boot process you can login. To hCollaboratione the system boot off the PRIMARY DISK you must reboot. You can simply enter the commands. "sync" and "reboot" and then let the system come up by itself.

6.2.9 Corrective Maintenance

Corrective maintenance for both secure and non-secure servers will be performed in accordance with licensing agreements.   administrators should be familiar for obtaining on-site technical support for both the non-secure and secure servers. administrators should also be familiar with obtaining phone support for both the non-secure and secure servers.

6.3 Emergency Procedures

What are the procedures at ?

6.3.1 Loss of Power

What are the procedures at ?

6.3.2 System Failures

In the event of a system failure, the SA should try to determine the problem. However, prior to attempting to repair any hardGOV Location Statere, the SA needs to determine if performing any repairs will void applicable GOV Location Staterranties or service agreements pertinent to the system. If the problem is beyond the SA's ability (i.e., a complete board failure), the administrator should call for on-site technical support.

What are procedures of problem notification and problem resolution?

6.3.3 Loss of Hard Drives

If a hard drive goes bad, such that the drive needs to be repld, the SA should perform actions to minimize the impact on overall operation. The HP internal disks and the HDS SAN disk drives hCollaboratione different hardGOV Location Statere level protection. Refer to the HP specific instructions and the HDS specific instructions.

6.3.4 Hitachi 9580 Storage Array

A. Hard Drives on Hitachi 9580 Storage Array

###NOTE NEEDED CLASSIFIED AND UNCLASSIFIED PROCEDURES

Hard drive locations in the storage array are as follows

#####INSERT STORAGE HARDGOV LOCATION STATERE LAYOUT

####INSERT LVM RECOVERY PROCEDURES

6.3.5 HEWLETT PACKARD 3440

The HEWLETT PACKARD 3440 has two (2) internal hard drives. The remaining hard drives are located on the storage array for a total of 14 hard drives

###INSERT HP DISK DIAGRAM HERE

7.0 BACKUP AND RECOVERY PROCEDURES

7.1 GOV PROGRAM HP Servers

The GOV PROGRAM database servers are physically located in sp provided by . The unclassified server for GOV PROGRAM receives information from data sources. The classified server for GOV PROGRAM obtains data through a Guard server

A full system backup of all system and database files will be performed upon system acceptance at each site and then upon each major system upgrade. FULL backups will also be performed on a quarterly basis. INCREMENTAL backups will be performed on the COLLABORATION data areas weekly.

Current specifications state **Veritas Netbackup** is the backup & restore utility of choice at .
Tapes from all backups at the sites will be kept in accordance with local directives. Tapes at the Reston Development site will be kept outside of the server room, and maintained for at least one year. The tapes at Reston will be kept in yet to be determined location in a safe.

7.2 Procedures for Creating a Full System Backup

###Determine and Specify

7.3 Procedures for Creating Incremental Backups

###Determine and Specify

7.4 DRP Copies of the GOV PROGRAM Systems

The backup tapes (full backup and weekly incremental) will be located at . interenal personnel will take responsibility for backups and the required backup schema. Netbackup is the current backup utility in use at , of which if implemented correctly and efficiciently can make up to four(4) copies with no additional licenses required. If choosed to purchase the functionality of additional copies then a simple additional license key for Netbackup GOV Location Stateult will allow to make up to ten (10) copies.

7.5 Restoration from Backup of the GOV PROGRAM Systems

####DETERMINE AND SPECIFY

8.0 IGNITE/UX INSTRUCTIONS

Ignite/UX is a very powerful system tool used for the system build and recovery of HPUX systems. The installing and the recovery of a system can be done both via a DAT tape(make_recovery) or over the Local Area Network (LAN)(make_net_recovery)

8.1 make_recovery & make_net_recovery INSTRUCTIONS

#make_net_recovery

The following process shows the routine to create a make_net_recovery archive on dlaas11 which is our IUX server. We will archive dladb02 & dladb03

1. **log in as root to dlaas11**

2. **Edit host file by insert dlaas03 and dladb02 into hosts**
   # vi /etc/hosts

```
 172.17.36.12    dlaas11
 172.17.36.4     dladb02
 172.17.36.5     dladb03
 127.0.0.1       localhost       loopback
```

3. **Edit .rhosts file**

```
vi /.rhosts
  dlaas02 root
```

4. **Create mountpoint /GOV Location Stater/opt/ignite/recovery/archives**

5. **Edit /etc/exports as follows**

```
      # vi /etc/exports
     /GOV Location Stater/opt/ignite/clients -anon=2
     /GOV Location Stater/opt/ignite/recovery/archives/dladb03 -
anon=2,access=dladb03
     /GOV Location Stater/opt/ignite/recovery/archives/dladb02 -
anon=2,access=dladb02
```

6. **Make directory**

```
#mkdir -p /GOV Location Stater/opt/ignite/recovery/archives/dlaas02
```

7. **Modify ownership**

```
      # chown bin:bin /GOV Location
Stater/opt/ignite/recovery/archives/dlaas02
```

8. **Export filesystems**

```
#exportfs -Collaboration
 re-exported /GOV Location Stater/opt/ignite/clients
 re-exported /GOV Location Stater/opt/ignite/recovery/archives/dladb03
 re-exported /GOV Location Stater/opt/ignite/recovery/archives/dladb02
```

9. **Make the archive from the client**

10. **Log in to dladb02 as root**

11. **Run make_net_recovery with the following options. The following output will be displayed.**

```
    ARCHIVE WILL TAKE ABOUT 30 minutes per machine,

  # make_net_recovery -s dlaas11 -x inc_entire=vg00
       * Creating NFS mount directories for configuration files.
GOV LOCATION STATERNING: /GOV Location
Stater/opt/ignite/recovery/client_mnt/dladb03 id not a symbolic link.
GOV LOCATION STATERNING: Failed creating symlink from clients lanic id to
clients hostname.
         File exists (errno = 17)

=======  07/09/04 16:53:58 EDT  Started make_net_recovery. (Fri Jul 09
16:53:58
         EDT 2004)
         @(#) Ignite-UX Revision B.5.1.33
         @(#) net_recovery (opt) $Revision: 10.618 $

       * Testing pax for needed patch
       * Passed pax tests.
       * Checking Versions of Recovery Tools
       * Creating System Configuration.
       * /opt/ignite/bin/sCollaboratione_config -f /GOV Location
Stater/opt/ignite/recovery/client_mnt/0x0
         0306E4B0BDB/recovery/2004-07-09,16:53/system_cfg vg00
       * Backing Up Volume Group /dev/vg00
       * /usr/sbin/vgcfgbackup /dev/vg00
Volume Group configuration for /dev/vg00 has been sCollaborationed in
/etc/lvmconf/vg00.con
f
       * Creating Map Files for Volume Group /dev/vg00
       * /usr/sbin/vgexport -p -m /etc/lvmconf/vg00.mapfile /dev/vg00
vgexport: Volume group "/dev/vg00" is still active.

       * Backing Up Volume Group /dev/vg01
       * /usr/sbin/vgcfgbackup /dev/vg01
Volume Group configuration for /dev/vg01 has been sCollaborationed in
/etc/lvmconf/vg01.con
f
       * Creating Map Files for Volume Group /dev/vg01
       * /usr/sbin/vgexport -p -m /etc/lvmconf/vg01.mapfile /dev/vg01
vgexport: Volume group "/dev/vg01" is still active.

       * Backing Up Volume Group /dev/vg02
       * /usr/sbin/vgcfgbackup /dev/vg02
Volume Group configuration for /dev/vg02 has been sCollaborationed in
/etc/lvmconf/vg02.con
f
       * Creating Map Files for Volume Group /dev/vg02
       * /usr/sbin/vgexport -p -m /etc/lvmconf/vg02.mapfile /dev/vg02
vgexport: Volume group "/dev/vg02" is still active.

       * Backing Up Volume Group /dev/vg04
       * /usr/sbin/vgcfgbackup /dev/vg04
Volume Group configuration for /dev/vg04 has been sCollaborationed in
/etc/lvmconf/vg04.con
f
       * Creating Map Files for Volume Group /dev/vg04
       * /usr/sbin/vgexport -p -m /etc/lvmconf/vg04.mapfile /dev/vg04
vgexport: Volume group "/dev/vg04" is still active.

       * Creating Control Configuration.
       * Creating Archive File List
       * Creating Archive Configuration

       * /opt/ignite/bin/make_arch_config -c /GOV Location
Stater/opt/ignite/recovery/client_mn
         t/0x00306E4B0BDB/recovery/2004-07-09,16:53/archive_cfg -g /GOV
Location Stater/opt/ign
         ite/recovery/client_mnt/0x00306E4B0BDB/recovery/2004-07-
09,16:53/flist
         -n 2004-07-09,16:53 -r 64 -d Recovery\ Archive -L
         /GOV Location Stater/opt/ignite/recovery/arch_mnt -l
         dlaas11:/GOV Location Stater/opt/ignite/recovery/archives/dladb03 -i
1 -m t
       * SCollaborationing the information about archive to
         /GOV Location Stater/opt/ignite/recovery/previews
       * Creating The Networking Archive

       * /opt/ignite/data/scripts/make_sys_image -d
         /GOV Location Stater/opt/ignite/recovery/arch_mnt -t n -s local -n
2004-07-09,16:53 -m
         t -w /GOV Location
Stater/opt/ignite/recovery/client_mnt/0x00306E4B0BDB/recovery/2004-
         07-09,16:53/recovery.log -u -R -g /GOV Location
Stater/opt/ignite/recovery/client_mnt/
         0x00306E4B0BDB/recovery/2004-07-09,16:53/flist -a 10087630

       * Preparing to create a system archive
       * The archive is estimated to reach 5043815 kbytes.
       * Free sp on /GOV Location Stater/opt/ignite/recovery/arch_mnt
         after archive should be about 83923641 kbytes.

      * Archiving contents of dladb03 via tar to
        /GOV Location Stater/opt/ignite/recovery/arch_mnt/2004-07-09,16:53.
      * Creation of system archive complete
NOTE:  The following files are in the list of files that were on the
      system, but they are no longer present.  These files are not
      included in the back-up:
      /GOV Location Stater/tmp/ign_configure/make_sys_image.log
      * Creating CINDEX Configuration File

      * /opt/ignite/bin/manage_index -q -c 2004-07-09,16:53\ Recovery\
Archive
        -i /GOV Location
Stater/opt/ignite/recovery/client_mnt/0x00306E4B0BDB/CINDEX -u
        Recovery\ Archive


======  07/09/04 17:31:17 EDT  make_net_recovery completed with GOV Location
Staternings



   12. Now verify the archive by logging to dlaas11

   13. cd /GOV Location Stater/opt/ignite/recovery/archives/dladb02

   14. Verify contents of dladb02 archive
# ls -la
total 9913136
drwxr-xr-x   2 bin        bin             96 Jul  9 15:34 .
drwxr-xr-x   5 root       root            96 Jul  9 15:12 ..
-rw-------   1 bin        sys       5075517029 Jul  9 16:22 2004-07-09,15:32
#

END
```

9.0 SECURITY ADMINISTRATION

Security of the Unix systems and the Oracle database is critical. Strict gulines must be followed.

9.1 GOV PROGRAM Security — Overview

COLLABORATION at is subject to security accreditation as defined in the DoD Directive 5200.28, “Security Requirements for Automated Information Systems,” and accreditation requirements. GOV PROGRAM is intended for operation in local area networks (LANs) that hCollaboratione been accredited by the s and that meet the requirements for connection to the DoD IP router networks, the NIPRNET, and the SECURE NETWORK. The security accreditation of is a management decision from , the designated approving authority (DAA), based on an analysis of the system’s security features, as well as security test and eGOV Location Stateluation (ST&E).

The GOV PROGRAM System Security Concept of Operations describes the security policy requirements of GOV PROGRAM and the security measures that are employed to satisfy these requirements. There are security measures enforced outs the computer system like physical access control procedures, but GOV PROGRAM also enforces automated security features including log-in and security auditing. Security Administration is a responsibility of the GOV PROGRAM SA, and the security of GOV PROGRAM depends on correct security administration. Security Administration includes user account management, password management, security auditing, managing operating system services and default settings. Additionally, security administration is also comprised of security-releGOV Location Statent routine operations, database security administration, administration of the secure guard (when this component is incorporated in the GOV PROGRAM system configuration), security monitoring, maintaining the accredited system configuration, managing communications connections, and other tasks as described in this manual.

GOV PROGRAM   operates in the "system-high" security mode of operation. All users are cleared to the highest level of security (classification) of the GOV PROGRAM   server they access (i.e., all users of GOV PROGRAM   on the Secret network hCollaboratione at least a Secret security clearance).

GOV PROGRAM   is implemented in a client-server configuration. The database server runs under a UNIX operating system that provs a "C2 level of trust," enforcing ntification, authentication, access control, and security auditing. Users access the database through a Web browser such as Netscape or Microsoft Internet Explorer.

The use of GOV PROGRAM   is authorized on a "need-to-know" and jobs requirements basis according to local policy. The GOV PROGRAM   log-in process requires the user to prov the user's name and password before access to the system is granted. Users can only query the GOV PROGRAM   database, download database query results to a file on disk, or print query results. The users are responsible for protecting information retrieved from the system.

GOV PROGRAM   softGOV Location Statere also provs a mechanism to ntify workstations that are connected to the classified server. Once ntified, the system does not allow the workstation's connection to the Unclassified server. The data on the Unclassified GOV PROGRAM   server is duplicated in the Secret server through a manual process using tape media or through a secure guard called the SECURE FTP APPLIANCE Guard. The SECURE FTP APPLIANCE guard allows for one GOV Location Statey data transfer electronically from the NIPRNET to the SECURE NETWORK.

9.2 Management of User Accounts

The SA(s) will operate within the operating system environment to establish and manage user accounts, to establish security auditing and other security parameters, and to implement programs that process the data received from source systems. Section 11 contains detailed instructions for creation of user accounts.

9.2.1 Establishing User Accounts

The SA will establish user accounts in the system for authorized personnel as determined by the proper command authority. System access will be authorized according to job requirements. GOV PROGRAM capability access control will ntify and authenticate all functional users. The log-in process will request user-id, password, and host IP address. The user ntity will be established positively before authorizing access. Connection to the system will be achieved if log-in is successful. Additionally, the system provs a mechanism by which it ntifies workstations connected to the classified server. Once ntified, the Unclassified server does not allow connection.

9.2.2 Processing User Account Requests

Individuals requiring access to the system will be authorized based upon a "need-to-know" according to job requirements. A user account will be established for each authorized user to a system. Individuals will obtain user account applications (sample at Appendix D). The individual who requires access to the Classified database server may also need access to the Unclassified server from an Unclassified user workstation. Because of location, the individual will hCollaboratione separate user accounts with different passwords on each system. The application will be submitted to Customer Support.   Customer Support will, in turn, process the application to the Systems Security Officer (SSO). The SSO will make the "need-to-know" determination. All approved applications will go to the SA for creation of a log-on and password. This information will be returned to the individual requesting access by a means consistent with the classification of the system information.

9.2.3 Deleting/Terminating User Accounts
Section 11 contains detailed instructions for the creation of user accounts.

9.2.4 Maintaining User Accounts
In order to obtain access to the GOV PROGRAM capability, users will be required to submit a request for access to the designated SA and must hCollaboratione GOV Location Statelid “need-to-know” requirements. The proper command management authority must approve this request for access. To access , users must hCollaboratione the GOV PROGRAM client softGOV Location Statere and a user account and password. Site policy will establish system administration requirements for user account management, password management (initial passwords, password selection, password change and expiration), log-in attempt control, security auditing and monitoring, system recovery and backup, and security incnt handling. Also, user site procedures will prov guidance and rules regarding user accounts, password management and protection, as well as security incnt and trouble reporting.

The servers, server consoles, and all user workstations will be appropriately marked for the classification of material being processed. The DoD GOV Location Staterning banner will be displayed before access to the system is granted. Since the system operates in the system-high mode of operation, magnetic media containing query results will be marked and protected according to the classification of the system and applicable security regulations. Printed data will bear the markings reflecting the classification of the system and will be protected to this level of classification according to applicable security regulations. Only the designated command authority can declare the actual classification of data in printed outputs or data sCollaborationed to magnetic media.

9.2.5 Initializing Discretionary Access Controls
The SA will maintain a security audit log of system access and user activity to ensure that all user activities are open to scrutiny and security monitoring. The security audit log or trail will keep a record of log-in and log-out activity, password changes, and other security-releGOV Location Statent user activities. The security audit mechanism will be kept running at all times.

9.2.6 Information Import
The GOV PROGRAM databases are populated with data from several DoD source databases. Data is sent to GOV PROGRAM using secure copy, FTP, or database-to database connectivity over the NIPRNET and the SECURE NETWORK. Anonymous FTP access to the GOV PROGRAM is not permitted. The GOV PROGRAM capability does not update any of the source data systems. Functional users can only query the GOV PROGRAM databases, sCollaboratione query results to a file on disk, or print query results. They are not provd capabilities to enter data or modify the GOV PROGRAM databases.

9.3 ntification and Authentication

9.3.1 User ID and Password Generation/Distribution
The designated SA will establish user accounts in the system for authorized personnel as determined by the proper command authority. System access will be authorized according to job requirements and a need to know. GOV PROGRAM capability access control will ntify and authenticate all functional users. Once the login and password hCollaboratione been generated, customer support will distribute account information consistent with the level of security of the server and in a manner compliant with local regulation.

The log-in process will request user-id, password, and host IP address. The user ntity will be established positively before access is authorized. Connection to the system will be achieved if log-in is successful. Additionally, the system provs a mechanism to ntify workstations connected to the classified server. Once it has ntified the Classified workstation, the Unclassified server does not allow connection. Access to is controlled through a log-in process requiring the user to prov user name and password before access is granted. The system also provs a mechanism by which it ntifies workstations that are connected to the classified server. Once it has ntified these workstations, the Unclassified server does not allow connection. Users can only query the databases, sCollaboratione query results to a file on disk, or print query results. The users are not provd capabilities to enter data or update the database.

9.3.2 Password Protection

When given an account to a server, the user or developer should be advised to change the password upon logging in, so no one knows the password but the user. The following rules apply when creating or changing passwords:

- Each password must hCollaboratione a minimum of eight characters.
- Characters must be from the seven-bit ASCII character set, and the letters must be from the English alphabet.
- Each password must contain at least one lowercase and one uppercase alphabetic characters and at least one numeric and one special character.
- Each password must differ from the user's log-in name and any reverse or circular shift of that log-in name. For comparison purposes, an uppercase letter and its corresponding lowercase equiGOV Location Statelent are treated as ntical.
- New passwords must differ from the old one by at least three characters. For comparison purposes, an uppercase letter and its corresponding lowercase equiGOV Location Statelent are treated as ntical.
- Do not make the password an easy word that can be guessed. Do not use man names, children's names, birthdays, or anniversaries.
- Do not use other information easily obtained about you. This includes license plate numbers, telephone numbers, social security numbers, the make of your automobile, the name of the street you live on, etc.
- Do not use a word contained in the English or foreign language dictionaries, spelling lists, or other lists of words.
- Everyone should change his or her password on a periodic basis (at least once a year, but every three months is preferable).

9.3.3 Login Attempt Control

On the Web application, if a user fails three times in a row to log in to correctly, will lock the user out. The user must then contact the help desk to request that the account be unlocked.

When a person telnets into the server, after five tries, the server will disconnect the log-in attempt, and send a message to the /GOV Location Stater/adm/messages file. The SA should check the file daily for any login failures and verify the IP address shown on the failure.

The SA should report any attempted break-ins to the command's Systems Security Officer and the Help Desk at GOV CONTRACTOR/PRIME CONTRACTOR in Reston, GOV LOCATION STATE, USA.

9.3.4 Password Aging

The user's password aging will be set in accordance with local directives. The SA will verify the requirements with the command's Systems Security Officer and set password aging accordingly.

9.3.5 System Time-Out

At present, the servers are not set for system time-outs. The SA should check to verify who is on the servers, and the date/time the person logged on. No users should be logged on overnight without the SA's knowledge and permission.

The servers will hCollaboratione TCP wrappers installed. TCP wrappers will allow the SA to monitor and filter incoming requests for SYSTAT, FINGER, FTP, EXEC, TALK and other network services. The SA can configure TCP wrappers to prevent any telnet sessions except those authorized in the hosts.allow file. Information on installing and configuring TCP wrappers can be found in the documentation accompanying the softGOV Location Statere.

9.4 Managing Operating System Services and Default Settings

The administrator will disable the anonymous FTP functions to prevent intruders from pulling data. The administrator should check the system logs daily to check for any attempted break-ins, and report such attempts accordingly.

System security parameters shall be updated as per local instructions.

9.5 Administration of the SECURE FTP APPLIANCE Security Guard

####INSERT WHEN APPLICABLE

9.6 Management, Administrative, and Procedural Controls

Physical Security of the GOV PROGRAM   database servers will operate from a secure facility. Physical access controls exist and are enforced by facility operators. Classified workstations will also operate from secure sps.

user training should cover security. Training stresses aGOV Location Statereness of security features and related procedures. A /   user security briefing, a user manual, an on-line tutorial, and system help are Collaborationailable. A / help desk should also be established in the future.

9.7 Network Communications

The classified system will run on a classified local area network. The classified database server will operate from a secure facility. Classified workstations will also operate from secure sps. Remote users of the classified system access it through a secure network, the SECURE NETWORK, which provs communications security (link encryption).

9.8 Reporting Security Incidents

Any security incnt (attempted intrusion, hacker attack, malicious softGOV Location Statere attack, etc.) affecting hosts should be reported expeditiously to the following individuals via e-mail or telephone:

Information System Security Manager
Technical Director
Security Engineer

10.0 OVERVIEW OF HP UNIX (HPUX)

HPUX is Hewlett Packards version of Open Systems Unix. The version initially installed at is HPUX 11.11

10.1 Installation

####

10.2 SoftGOV Location Statere Installation

#####

10.3 Patch Installation

Patches can be installed indivually as a single patch or as a “bundle”

####INSERT PATCH INSTRUCTIONS

10.4 Kernal Parameters

#####

10.5 Performance Issues

11.0 HIGH COLLABORATIONAILABILITY (HA) CLUSTERS

A highly Collaborationailable cluster will allow an application service to continue to run in the event of hardGOV Location Statere or softGOV Location Statere failure. chose MC/ServiceGuard to prov this capability.

###INSERT DIAGRAM

11.1 MC/ServiceGuard Overview & Architecture

MC/ServiceGuard is a softGOV Location Statere product developed by HP for HP 9000 Series 800 computer systems.
This product allows you to create highly Collaborationailable clusters of which will allow the application to continue to run in the event of a hardGOV Location Statere or softGOV Location Statere failure.

This product is an “optional product” and will require a separate license to run. However, with the Mission Critical Operating Environment it includes a fully licensed product.

This document certainly won’t make you and expert in MC/ServiceGuard. Please refer to HP Document “Managing MC/ServiceGuard” for more detailed instructions.

Basic Architecture

SoftGOV Location Statere Compenents of MC/ServiceGuard

1. Package Manager

2. Cluster Manager

3. Network Manager

####INSERT DIAGRAM

11.1.2 MC/ServiceGuard Daemons and Processes.

There are nine daemon processes associated with MC/ServiceGuard.

PROCESS	DESCRIPTION
/usr/lbin/cmclconfd	ServiceGuard configuration daemon
/usr/lbin/cmcld	ServiceGuard cluster daemon
/usr/lbin/cmlogd	ServiceGuard Syslog log daemon
/usr/lbin/cmlvmd	Cluster Logical Volume manager daemon
/opt/cmom/lbin/cmomd	Cluster object manager daemon
/usr/lbin/cmsnmpd	Cluster SNMP subagent
/usr/lbin/cmsrGOV Location Statessistd	ServiceGuard Service Assist daemon
/usr/lbin/cmtaped	ServiceGuard shared tape daemon
/usr/lbin/qs	ServiceGuard Quorum server daemon

11.2 Installation of MC/ServiceGuard

##INSERT INFORMATION HERE

11.3 Configuration of MC/ServiceGuard

###Insert info here

11.3.1 Package & Cluster Planning

###

11.3.2 Package and Cluster Testing (FAILOVER)

####Insert failover testing procedures here

11.3.3 MC/Service Guard Configuration Files

####Insert Config Files here

11.3.4 ServiceGuard Extension For RAC

This product is a required additional product that integrates Oracle Real Application Clusters into MC/ServiceGuard. The additional daemon below is added when this Extension product is installed.

PROCESS	DESCRIPTION
/usr/lbin/cmgmsd	Group membership daemon for RAC

11.3.4.1 Installation of ServiceGuard for RAC

##Insert Instructions

11.4 Installation of MirrorDisk/UX

MirrorDisk/UX is important part of HA clusters. Installation and configuration of both internal HP disks will be required.

MirrorDisk/UX is an optional product that is utilized for mirroring Logical Volume Manager(LVM) disks on HPUX platforms. This product is extremely easy to use and can be administered though command line and SAM.(Note, SAM can not create a "bootable" mirror). We will document the command line process.

Below are the instructions to mirror the primary disk filesystems and sGOV Location Statep. In this configuration we only hCollaboratione two disks and one Volume Group. The primary disks will be mirrored to secondary disk in the Volume Group 00 (VG00)

EXTEND VOLUME GROUP

1. Determine the device file of the secondary disk. Ioscan is the perfect command for this.

```
# ioscan -fnC disk

Class      I  H/W Path       Driver  S/W State   H/W Type     Description

========================================================================

disk       0  0/0/2/0.0.0.0  sdisk   CLAIMED     DEVICE       TEAC    DV-28E-C

                            /dev/dsk/c0t0d0   /dev/rdsk/c0t0d0

disk       1  0/1/1/0.0.0    sdisk   CLAIMED     DEVICE       HP
73.4GST373453LC

                            /dev/dsk/c2t0d0   /dev/rdsk/c2t0d0

disk       2  0/1/1/0.1.0    sdisk   CLAIMED     DEVICE       HP
73.4GST373453LC

                            /dev/dsk/c2t1d0   /dev/rdsk/c2t1d0
```

2. Verify vg00 configuration. You will notice that there is one Physical Volume (PV).

```
# vgdisplay -v vg00


--- Volume groups ---

VG Name                     /dev/vg00

VG Write Access             read/write

VG Status                   Collaborationailable

Max LV                      255

Cur LV                      8

Open LV                     8

Max PV                      16

Cur PV                      1

Act PV                      1

Max PE per PV               4384
```

```
VGDA                        2
PE Size (Mbytes)            16
Total PE                    4374
Alloc PE                    853

Free PE                     3521
Total PVG                   0
Total Spare PVs             0
Total Spare PVs in use      0


   --- Logical volumes ---
   LV Name                     /dev/vg00/lvol1
   LV Status                   Collaborationailable/syncd

Standard input
   LV Size (Mbytes)            304
   Current LE                  19
   Allocated PE                19
   Used PV                     1


   LV Name                     /dev/vg00/lvol2
   LV Status                   Collaborationailable/syncd
   LV Size (Mbytes)            4096
   Current LE                  256
   Allocated PE                256
   Used PV                     1


   LV Name                     /dev/vg00/lvol3
   LV Status                   Collaborationailable/syncd
   LV Size (Mbytes)            208
   Current LE                  13
   Allocated PE                13
   Used PV                     1

   LV Name                     /dev/vg00/lvol4
   LV Status                   Collaborationailable/syncd
   LV Size (Mbytes)            208
   Current LE                  13
Standard input
   Allocated PE                13
Standard input
   Used PV                     1

   LV Name                     /dev/vg00/lvol5
   LV Status                   Collaborationailable/syncd
   LV Size (Mbytes)            32
   Current LE                  2
   Allocated PE                2
   Used PV                     1

   LV Name                     /dev/vg00/lvol6
   LV Status                   Collaborationailable/syncd
   LV Size (Mbytes)            2192
   Current LE                  137
   Allocated PE                137
   Used PV                     1
   LV Name                      /dev/vg00/lvol7

   LV Status                    Collaborationailable/syncd

   LV Size (Mbytes)             2000

   Current LE                   125

   Allocated PE                 125

   Used PV                      1



Standard input

   LV Name                      /dev/vg00/lvol8

Standard input

   LV Status                    Collaborationailable/syncd

   LV Size (Mbytes)             4608

   Current LE                   288

   Allocated PE                 288

   Used PV                      1



   --- Physical volumes ---

   PV Name                      /dev/dsk/c2t0d0

   PV Status                    Collaborationailable

   Total PE                     4374

   Free PE                      3521

   Autoswitch                   On
```

3. Create a Physical Volume on the secondary disk /dev/dsk/c2t1d0.

```
# pvcreate -B /dev/rdsk/c2t1d0

Physical volume "/dev/rdsk/c2t1d0" has been successfully created.
```

4. Extend the volume group vg00 with the new physical volume.

```
# vgextend /dev/vg00 /dev/dsk/c2t1d0

Volume group "/dev/vg00" has been successfully extended.

Volume Group configuration for /dev/vg00 has been sCollaborationed in
/etc/lvmconf/vg00.conf
```

5. Pl boot utilities on disk

```
# mkboot /dev/rdsk/c2t1d0
```

6. Add the AUTO file to the boot LIF

```
# mkboot -a "hpux -lq /stand/vmunix" /dev/rdsk/c2t1d0
```

7. Review the Filesystem layout(specifically the lvols)

```
# bdf

Filesystem          kbytes    used   Collaborationail %used Mounted on

/dev/vg00/lvol3     212992   88416  123648   42% /

/dev/vg00/lvol1     298928   41384  227648   15% /stand

/dev/vg00/lvol8    4718592  402984 4282296    9% /GOV Location Stater

/dev/vg00/lvol7    2048000 1144704  896248   56% /usr

/dev/vg00/lvol4     212992    2464  208952    1% /tmp

/dev/vg00/lvol6    2244608 1611232  628440   72% /opt

/dev/vg00/lvol5      32768    2392   30152    7% /home

dccsofs04.agc.local:/vol/proj/sudo

                   915941648 823250224 92691424   90% /usr/local/sudo
```

8. Review the sGOV Location Statepinfo and verify lvol

```
# sGOV Location Statepinfo

             Kb      Kb      Kb   PCT  START/      Kb

TYPE      COLLABORATIONAIL    USED    FREE  USED   LIMIT RESERVE  PRI  NAME

dev     4194304       0 4194304    0%       0       -    1  /dev/vg00/lvol2
```

```
reserve       -  172720 -172720
memory  1568380  180988 1387392   12%
```

EXTEND LOGICAL VOLUMES

9. Extend the logical volumes. (lvols) You must run lvextend for each logical volume. There are eight total.

```
# lvextend -m 1 /dev/vg00/lvol1 /dev/dsk/c2t1d0

The newly allocated mirrors are now being synchronized. This operation will

take some time. Please GOV Location Stateit ....

Logical volume "/dev/vg00/lvol1" has been successfully extended.

Volume Group configuration for /dev/vg00 has been sCollaborationed in
/etc/lvmconf/vg00.conf


# lvextend -m 1 /dev/vg00/lvol2 /dev/dsk/c2t1d0

The newly allocated mirrors are now being synchronized. This operation will

take some time. Please GOV Location Stateit ....

Logical volume "/dev/vg00/lvol2" has been successfully extended.

Volume Group configuration for /dev/vg00 has been sCollaborationed in
/etc/lvmconf/vg00.conf



# lvextend -m 1 /dev/vg00/lvol3 /dev/dsk/c2t1d0

The newly allocated mirrors are now being synchronized. This operation will

take some time. Please GOV Location Stateit ....

Logical volume "/dev/vg00/lvol3" has been successfully extended.

Volume Group configuration for /dev/vg00 has been sCollaborationed in
/etc/lvmconf/vg00.conf


# lvextend -m 1 /dev/vg00/lvol4 /dev/dsk/c2t1d0

The newly allocated mirrors are now being synchronized. This operation will

take some time. Please GOV Location Stateit ....

Logical volume "/dev/vg00/lvol4" has been successfully extended.
```

```
Volume Group configuration for /dev/vg00 has been sCollaborationed in
/etc/lvmconf/vg00.conf


# lvextend -m 1 /dev/vg00/lvol5 /dev/dsk/c2t1d0

The newly allocated mirrors are now being synchronized. This operation will

take some time. Please GOV Location Stateit ....

Logical volume "/dev/vg00/lvol5" has been successfully extended.

Volume Group configuration for /dev/vg00 has been sCollaborationed in
/etc/lvmconf/vg00.conf


# lvextend -m 1 /dev/vg00/lvol6 /dev/dsk/c2t1d0

The newly allocated mirrors are now being synchronized. This operation will

take some time. Please GOV Location Stateit ....

Logical volume "/dev/vg00/lvol6" has been successfully extended.

Volume Group configuration for /dev/vg00 has been sCollaborationed in
/etc/lvmconf/vg00.conf


# lvextend -m 1 /dev/vg00/lvol7 /dev/dsk/c2t1d0

The newly allocated mirrors are now being synchronized. This operation will

take some time. Please GOV Location Stateit ....

Logical volume "/dev/vg00/lvol7" has been successfully extended.

Volume Group configuration for /dev/vg00 has been sCollaborationed in
/etc/lvmconf/vg00.conf


# lvextend -m 1 /dev/vg00/lvol8 /dev/dsk/c2t1d0

The newly allocated mirrors are now being synchronized. This operation will

take some time. Please GOV Location Stateit ....

Logical volume "/dev/vg00/lvol8" has been successfully extended.

Volume Group configuration for /dev/vg00 has been sCollaborationed in
/etc/lvmconf/vg00.conf
```

VERIFY CONFIGURATION

10. Verify the boot information.

```
#lvlnboot -v
```

```
Boot Definitions for Volume Group /dev/vg00:
Physical Volumes belonging in Root Volume Group:
        /dev/dsk/c2t0d0 (0/1/1/0.0.0) -- Boot Disk
        /dev/dsk/c2t1d0 (0/1/1/0.1.0) -- Boot Disk
Boot: lvol1     on:     /dev/dsk/c2t0d0
                        /dev/dsk/c2t1d0
Root: lvol3     on:     /dev/dsk/c2t0d0
                        /dev/dsk/c2t1d0
SGOV Location Statep: lvol2     on:     /dev/dsk/c2t0d0
                        /dev/dsk/c2t1d0
Dump: lvol2     on:     /dev/dsk/c2t0d0, 0
```

11. Verify the updated vg00 physical volumes.

```
# vgdisplay -v vg00
--- Volume groups ---
VG Name                     /dev/vg00
VG Write Access             read/write
VG Status                   Collaborationailable
Max LV                      255
Cur LV                      8
Open LV                     8
Max PV                      16
Cur PV                      2
Act PV                      2
Max PE per PV               4384
VGDA                        4
PE Size (Mbytes)            16
Total PE                    8748
Alloc PE                    1706
```

```
Free PE                     7042
Total PVG                   0
Total Spare PVs             0
Total Spare PVs in use      0

   --- Logical volumes ---
   LV Name                     /dev/vg00/lvol1
   LV Status                   Collaborationailable/syncd
   LV Size (Mbytes)            304
   Current LE                  19
   Allocated PE                38
   Used PV                     2

   LV Name                     /dev/vg00/lvol2
   LV Status                   Collaborationailable/syncd
   LV Size (Mbytes)            4096
   Current LE                  256
   Allocated PE                512
   Used PV                     2

   LV Name                     /dev/vg00/lvol3
   LV Status                   Collaborationailable/syncd
   LV Size (Mbytes)            208
   Current LE                  13
   Allocated PE                26
   Used PV                     2

   LV Name                     /dev/vg00/lvol4
   LV Status                   Collaborationailable/syncd
   LV Size (Mbytes)            208
   Current LE                  13
   Allocated PE                26
   Used PV                     2

   LV Name                     /dev/vg00/lvol5
   LV Status                   Collaborationailable/syncd
   LV Size (Mbytes)            32
   Current LE                  2
   Allocated PE                4
   Used PV                     2

   LV Name                     /dev/vg00/lvol6
   LV Status                   Collaborationailable/syncd
   LV Size (Mbytes)            2192
   Current LE                  137
   Allocated PE                274
   Used PV                     2

   LV Name                     /dev/vg00/lvol7
   LV Status                   Collaborationailable/syncd
   LV Size (Mbytes)            2000
   Current LE                  125
   Allocated PE                250
   Used PV                     2

   LV Name                     /dev/vg00/lvol8
```

```
   LV Status                   Collaborationailable/syncd

   LV Size (Mbytes)            4608

   Current LE                  288

   Allocated PE                576

   Used PV                     2



   --- Physical volumes ---

   PV Name                     /dev/dsk/c2t0d0

   PV Status                   Collaborationailable

   Total PE                    4374

   Free PE                     3521

   Autoswitch                  On


   PV Name                     /dev/dsk/c2t1d0

   PV Status                   Collaborationailable

   Total PE                    4374

   Free PE                     3521

   Autoswitch                  On
```

TEST THE MIRROR

To test the mirror we need to reboot and boot of the newly created mirror.

12. Enter "reboot" . System will reboot and allow you to interrupt the boot process.

13. Ensure you are on a system console. Enter login info.

```
MP password: *****


MP login: Admin
MP password: *****
```

```
                     Hewlett-Packard Management Processor

    (c) Copyright Hewlett-Packard Company 1999-2003.  All Rights Reserved.

                           MP Host Name: uninitialized

                              Revision E.02.26

*************************************************************************
                        MP ACCESS IS NOT SECURE
 Default MP users are currently configured and remote access is enabled.
 Modify default users passwords or delete default users (see UC command)
                                   OR
           Disable all types of remote access (see SA command)
*************************************************************************


   MP MAIN MENU:

         CO: Console
        VFP: Virtual Front Panel
         CM: Command Menu
         CL: Console Log
         SL: Show Event Logs
        CSP: Connect to Service Processor
         SE: Enter OS Session
         HE: Main Help Menu
          X: Exit Connection

[uninitialized] MP> co



        (Use Ctrl-B to return to MP main menu.)



- - - - - - - - - - Prior Console Output - - - - - - - - - -
Closing open logical volumes...
Done



FirmGOV Location Statere Version  44.6

Duplex Console IO Dependent Code (IODC) revision 1



- - - - - - - - - - - - Live Console - - - - - - - - - - - -
```

14. Now you must stop boot process by selecting any key. Follow the RED commands and enter at the appropriate prompts.

```
FirmGOV Location Statere Version  44.6
```

```
Duplex Console IO Dependent Code (IODC) revision 1
-------------------------------------------------------------------------------
-
   (c) Copyright 1995-2004, Hewlett-Packard Company, All rights reserved
-------------------------------------------------------------------------------
-

  Processor   Speed            State           CoProcessor State  Cache Size
  Number                                       State              Inst
Data
  ---------  --------   ---------------------  -----------------  -----------
-
      0      800  MHz   Active                 Functional         33554432
33552
      1      800  MHz   Idle                   Functional         33554432
33552

  Central Bus Speed (in MHz)  :        200
  Collaborationailable Memory            :    2097152  KB
  Good Memory Required        : Not initialized. Defaults to 32 MB.

   Primary boot path:    0/1/1/0.0
   Alternate boot path:  0/0/2/0.3
   Console path:         0/7/1/1.0
   Keyboard path:        0/0/4/0.0


Processor is booting from the first Collaborationailable device.

To discontinue, press any key within 10 seconds.

Boot terminated.
```

15. At the following "Main Menu" :Enter command or menu: interf below we must specify the boot device. We can find Collaborationailable boot devices by entering the "SEA" command. You can also use the "CO" command to view current boot GOV Location Statelues set in memory.

```
---- Main Menu ---------------------------------------------------------------
-

     Command                           Description
     -------                           -----------
     BOot [PRI|ALT|<path>]             Boot from specified path
     PAth [PRI|ALT] [<path>]           Display or modify a path
     SEArch [DIsplay|IPL] [<path>]     Search for boot devices

     COnfiguration menu                Displays or sets boot GOV Location
Statelues
     INformation menu                  Displays hardGOV Location Statere
information
     SERvice menu                      Displays service commands

     DIsplay                           Redisplay the current menu
     HElp [<menu>|<command>]           Display help for menu or command
     RESET                             Restart the system
----
```

```
Main Menu: Enter command or menu > sea

Searching for potential boot device(s)
This may take several minutes.

To discontinue search, press any key (termination may not be immediate).



IODC
   Path#  Device Path (dec)  Device Path (mnem)  Device Type
Rev
   -----  -----------------  ------------------  -----------               --
--
   P0     0/0/2/0.0          .0                Random access media       0
   P1     0/1/1/0.1          intscsia.1           Random access media       0
   P2     0/1/1/0.0          intscsia.0           Random access media       0
   P3     0/3/1/0.0                               Random access media       6
   P4     0/4/1/0.0                               Random access media       6


Main Menu: Enter command or menu > bo p2

Interact with IPL (Y, N, or Cancel)?> y
Booting...
Boot IO Dependent Code (IODC) revision 0


HARD Booted.

ISL Revision A.00.43  Apr 12, 2000

ISL>
```

16. Now at the ISL> prompt enter the command to boot."hpux"

```
ISL> hpux
Boot
: disk(0/1/1/0.0.0.0.0.0.0;0)/stand/vmunix
10964992 + 2052096 + 1419600 start 0x1f77e8




alloc_pdc_pages: Relocating PDC from 0xffffff0f0c00000 to 0x3f900000.
```

17. System will continue its boot process. At the completion of the boot process you can login. To hCollaboratione the system boot off the PRIMARY DISK you must reboot. You can simply enter the commands. "sync" and "reboot" and then let the system come up by itself.

END OR MIRRORDISK INSTRUCTIONS

12.0 HPUX SoftGOV Location Statere and Patch Instructions

Installing patches and softGOV Location Statere is a routine part of HP systems administration.

Explain HP softGOV Location Statere structure
Bundle
Filesets
Files

12.1 HPUX SoftGOV Location Statere Installation (SWINSTALL)

####Insert swinstall Instructions

12.2 HPUX Patch Installation

###Explain HP patching structure
##Insert Patching Instructions
###Download or Cdrom
###Swinstall

12.3 HPUX SoftGOV Location Statere Depot Instructions

####Insert Instructions

13.0 HPUX Specific Utilities and Tools

HPUX has many utilities and tools that aid in the administration of the HPUX servers.

13.1 SAM (System Administration Manager)

###(Basic Instructions and Snapshots)

13.2 Diagnostics

##ODE (Online Diagnostics overview)
###(Basic Instructions and Snapshots)

13.3 MeasureGOV Location Statere

#######(Basic Instructions and Snapshots)

13.4 GLANCE

########(Basic Instructions and Snapshots)

14. GUARD

####Insert Guard info

15.0 SERVER SECURITY AND HARDENING

During the course of events, the system archetecture underwent a security eGOV Location Stateluation. While the actual results of the security eGOV Location Statelaution are classified (due to areas discussed on a secret server), many server packages and service ports open that could allow a hacker access to the server were found. Part of the DISA Security Technical Implementation Gu (STIG) recommends removing unnecessary packages from the servers, and shutting down service ports that are not used.

The procedure used for the server security hardening GOV Location States created using the DISA Security Technical Implementation Gu.

As from performing the server hardening, the SA will check periodically that all portions of the security hardening are being maintained. Anything not conforming to the procedure will be fixed immediteally.

15.1 Server SoftGOV Location Statere Bundles

A listing of the packages not normally needed for to run GOV Location States compiled. The following is the listing of packages to be removed. Packages should be removed in the order of application (app) or ALE first, then the system (sys) packages. While some sites may not hCollaboratione certain packages installed, this list attempts to list all packages that servers do not need. The LSM packages are installed from the Oracle 9i RAC 8i installation. The SA must know what packages are being used on the servers prior to removing any server package.

If the SA finds that a certain server packages are required to support operations (example gcc), then do not remove the package. Instead keep the package and inform Reston with a justification of why the package GOV Location States not removed (example: gcc package maintained on server to support Tripwire)

##########INSERT SWLIST HERE###

15.2 Inetd.conf File

The SA will edit the /etc/inetd.conf file to comment out the services not used. Changes from the file shown below are acceptable with justifications. An example is if there is no printing services for the server, then the printer daemon can be commented out. However, differences must be documented and sent to Reston for maintaining the server configuration matrix.

**************** START OF INETD.CONF ************************

************************ END OF INETD.CONF **************************

15.3 UMASK

The DISA STIG has the requirement to set the system umask to 037.

However, the HPUX Security Gu has a discussion to set root's umask to 077 to further prevent hackers from altering files created by root. To accomplish setting the umask, the SA will need to perform the following:

Edit the /etc/default/login file, and change the umask line to read UMASK=027.

Edit root's .profile and insert the line, "umask 077".

Edit the /etc/profile file and set the umask to 027.

Edit the /etc/skel/local.cshrc file and set the umask to 027.

15.4 Startup Files

The DISA STIG states that all user's startup files (.profile, .login, and .cshrc) shall be owned by root and hCollaboratione the permission of 640. The SA must also ensure the group is GOV Location Statelid for each user so they can read their startup file. To change the permission and ownership, the SA will run the following commands:

```
find / -name .profile -exec chmod -R 640 {} \;
find / -name .profile -exec chown -R root {} \;
find / -name .login -exec chmod -R 640 {} \;
find / -name .login -exec chown -R root {} \;
find / -name .cshrc -exec chmod -R 640 {} \;
find / -name .cshrc -exec chown -R root {} \;
```

The exception to above is root's .profile. The permission on root's .profile will be 500. This is set by "chmod 500 .profile" in root's home directory.

15.5 Home Directories

The UNIX STIG discusses the requirements for home directories. The home directory contains user's files and exists for the user's exclusive use. All files in and subordinate to, the directory will be owned by the owner (exception is the startup files being owned by root). The requirements of the home directories are:

❑ Each user will be assigned a home directory in the /etc/passwd file.

❑ All home directories defined in the /etc/passwd file will exist.

- User home directories will hCollaboratione permissions of 700, and never more permissive then 750.

- The UID of a user’s home directory will be that of the user.

- The gid of a user’s home directory will be the user’s primary gid.

All users' home directories will be located in (TBD). Logins that will not be located in (TBD) are as follows:

Login	**Home Directory**
TBD	

To ensure the above requirements, the SA will run the pwck to check GOV Location Statelid home directories and fix any
discrepancies.

All home directories will hCollaboratione the permissions of 750 to allow group read access for selected files. The exceptions are root’s home directory (that will hCollaboratione a permission of 700) and the datafeed home directories (that will hCollaboratione a permission of 775). To perform this, the SA will perform the following commands:

```
chmod 700 /root
cd /h/USERS
chmod 750 *
```

The SA will verify that user is the only owner of the files in their home directory. The exception to this is the startup files being owned by root. The SA needs to go into each user's home directory and check the ownership of the files and fix any discrepancies.

The datafeed home directories will hCollaboratione a UID of dba and a GID of datafeeds. This will allow dba to be able to load the data from the source systems into the database.

15.6 Shells

Only authorized shells will be used on the servers. The default shells allowed will be listed in the /etc/shells file. This file will contain the following lines:

```
/usr/bin/sh
/bin/sh
/usr/bin/ksh
/bin/ksh
/usr/bin/csh
/bin/csh
/sbin/sh
```

15.7 System Accounts

The SA will edit the /etc/passwd file to make certain system accounts use the /usr/bin/false shell. This will prevent unGOV Location Statented ftp access to the server from the accounts.

The /etc/passwd file will read as follows for system accounts:

######INSERT /ETC/PASSWD HERE

15.8 Device Files

The UNIX STIG states to disable world-readable and world-writable access to prevent the devices from being compromised. To perform this, the SA will change the pty* and tty* permissions to 600 in the /dev/pseudo directory. The SA can perform this be doing the following:

```
cd /dev/pseudo
chmod 600 ptc@0:pty*
chmod 600 ptsl@0:tty
```

NOTE: The second chmod is on ptsl (papa-tango-sierra-lima).

15.9 Special Purpose Access Modes

Special operating characteristics may be assigned to a file or directory. These special characteristics are:

set-user-id (suid)
set-group-id (sgid)
set sticky-bit

The SA will verify that the files suid_perms and sgid_perms are located in /security1. These files maintain a listing of all files that hCollaboratione the suid or sgid characteristics set. If not, create these files by running the following:

```
cd /security1
find / -perm 4000 -exec ls -l {} \; > suid_perms
find / -perm 2000 -exec ls -l {} \; > sgid_perms
```

The SA will check periodically that there are no additional files from those listed in the above files. If any found, the SA will verify that the file requires the characteristic and handle the file as needed.

15.10 Boot Security Mode

#### INSERT SECURITY MODE HERE INSTRUCTIONS

15.11 Login File

The SA will make the following changes to the /etc/default/login file.

Uncomment the line CONSOLE=/dev/console

This only allows root to login at the console.

```
Change the umask line to read UMASK=027
```

This sets the system umask for anyone logging on to 027.

```
Uncomment the timeout line and change it to read TIMEOUT=900
```

This sets the amount of time to 15 minutes before abandoning an idle login session.

15.12 Secure Shell Parameters

The SA will edit the /etc/sshd config file to ensure of security. Change the file for the lines to read as follows:

```
PermitRootLogins no
PrintMotd yes
```

15.13 Unowned Files

The SA will check that there are no unowned files. Any unowned files found will need to hCollaboratione the ownership changed (chown) or removed from the server. To find any unowned files, perform the following command:

```
find / -nouser -o -nogroup
```

15.14 File Transfer Protocol

The SA will create a banner for ftp logins by creating the file /etc/default/ftpd. The contents of this file will be:

```
BANNER="This is a DOD computer system. Use of this DoD computer system, authorized or
unauthorized, constitutes consent to monitoring of this system."
```

NOTE: The text in the banner must be in one continuous line.

The SA will create an /etc/ftpusers file. This file will list the usernames of users not allowed to use ftp. The owner of the file will be root. The ftpusers file will contain the following logins:

```
root
daemon
bin
sys
adm
lp
smtp
uucp
```

nuucp
listen

Perform "chmod 640 ftpusers" to set the permission on the file.

15.15 Remote Login (rlogin and rsh)

Remove logins from rlogin and rsh are not permitted. Also, there will be no .rhosts file on the system. The SA will check for any .rhosts files by running the following command.

```
find / -name .rhosts
```

If any .rhosts files are found, the SA must remove them.

15.16 CRON Access

The cron is a scheduling utility. It controls jobs configured to run in the background on a recurring schedule. Cron determines the schedule and the jobs from configuration files called crontabs. It keeps track of each specific crontab creator and executes the programs with the privileges of the crontab creator. Because of that, crontab entries will not execute world or group writable programs.

The SA will review all cron jobs by reading the cron file of every system account in /GOV Location Stater/spool/cron/crontabs. Ensure all cron activities are logged by setting "CRONLOG=yes" in /etc/default/cron.

The cron.allow and at.allow files contain the logins that are permitted to use the cron and at commands. The cron.deny and at.deny files contain the logins that are not permitted to use the cron and at commands. The SA will verify the existance of the following files under /etc/cron.d

cron.allow
cron.deny
at.allow
at.deny

The cron.allow file will contain the logins permitted to use the cron. Other than the DBAs and SAs at the site, the list will be limited to:

root

###DETERMINE
The at.allow file will contain the following logins

####DETERMINE
The cron.deny and at.deny will contain the following logins:

###DETERMINE

15.17 Core Files

The operating system writes out a core image of a process when it is terminated due to the receipt of some signals. The core image is called core and is written in the process's working directory (provd it can be;

normal access controls apply). A process with an effective user ID different from the real user ID will not produce a core image.

The core file contains all the process information pertinent to debugging: contents of hardGOV Location Statere registers, process status, and process data. The format of a core file is object file specific. The problem with the core file is that it also contains the login and password in clear text.

The SA will search the server for any core files. Check if the core file has any GOV Location Statelidation, then remove the core file from the server. Use the following commands to search for core files:

```
cd /
find / -name core* -print
```

NOTE: During the search, the SA will find core directories, these are acceptable and required for softGOV Location Statere to run properly.

15.18 RPC

####INSERT RPC INFO HERE

15.19 TCP Sequencing

##### INSERT TCP CONFIG INFO

15.20 Auditing

Auditing ensures that users are accountable for their actions. Auditing allows the detection of prtential security problems and suspicious patterns, and tr actions to specific users. HPUX uses softGOV Location Statere referred to as the C2 Security Module (SM) to implement auditing.

The DISA STIG states that as a minimum, the following flags will be audited:

lo – audits logins and logouts
fc – audits failed file creations
fd – audits failed file deletions
ad – audits all administrative actions
pc – audits process operations, such as fork, exec, and exits
ex – audits executed programs
fr – audits all failed file writes
fm – audits all failed file modifications, such as failed chowns and chmods
fw – audits all file writes

To start the auditing process, the SA will perform the following:

##INSERT INSTRUCTIONS FOR C2 AUDITING

The SA will set up a crontab to cycle the audit logs every night. Perform the following commands as root:

##INSERT CRONTAB

15.21 Syslog

The system logging daemon (syslogd) reads and forGOV Location Staterds system messages to the log files and/or users. Malicious users can flood the logging daemon with unauthorized messages unless syslogd is configured to accept messages only from designated hosts.

Servers will hCollaboratione the system name in the /etc/hosts file, and hCollaboratione loghost as an alias.

The SA will set up the syslog by editing the /etc/syslog.conf file. The file should read as follows:

#### INSERT SYSLOG.CONF

The SA will review the logs daily. The SA will clean up the logs on a daily basis.

15.22 File and Directory Permissions

The most important part of security and Configuration Management is the permissions of the directories and files on the servers. All Servers will follow the listing of the file and directory permissons as shown in Appendix _X_.

The SA is requred to check the permissions on the server and fix any descrepancies.

15.23 Passwords

The DISA STIG provides many guidelines on passwords. These are:

- ❑ Each entry in the /etc/passwd file will hide a password assigned of will be disabled.
- ❑ Passwords will be a mininum of 8 characters in length, hCollaboratione one uppercase, one lowercase, one numeric, and one special character.
- ❑ Passwords will not contain personal information such as names, telephone numbers, account names, dictionaty words, etc.
- ❑ Passwords will not contain consecutively repeating characters.
- ❑ User passwords will be changed every 90 days.
- ❑ Passwords will not be reuserd within ten password changes.
- ❑ Application passwords will be changed at least once a year and anytime an application administrator is reassigned.
- ❑ Users will not be allowed to change their passwords more than once every 24 hours.

□ The root password will be changed on the same 90 day schedule as for users.

□ The root password will be changed whenever someone who knows the root password is reassigned.

□ The number of people who know the root password will be strictly limited.

To accommodate the password aging on the Unix System, the SA will start up the System Administration Manager (sam).. Each user login will be edited to follow the requirements of password aging. These rules will apply unless overridden by local directives.

Root and User logins

Min Change	1 day
Max Change	90 days
Max Inactive	180 days
GOV Location Staterning	10 days

Application logins

Min Change	1 day
Max Change	365 days
GOV Location Staterning	10 days

The datafeed and push logins will be changed on a coordinated basis from the datafeed coordinator. Do not set the password aging on these logins.

NOTE: The SA will need to reset the passwords for dba and web1 after setting password aging. If this is not done, database processing and web queries will not work.

15.24 SUDO

Sudo is a security tool which allows users to move between accounts without knowing the specific password for that account. The user controls are administered by editing the /etc/sudoers file.

Sudo is installed from the mount. /usr/local/sudo/sudo-1.6.6

ACCESS: REQUIRES ROOT ACCESS

INSTALLATION TIME: 20 minutes.

REBOOT: NO

DEPENDENCIES: CC Compiler

INSTALLATION AND CONFIGURATION

1. Run the configure Script. The default for install of HPUX does not hCollaboratione the ANSI CC compiler.

(Install is started by running the configuration script. This script will compile and then install sudo. The script will also install the configuration file /etc/sudoers and the /GOV Location Stater/run/sudo directory)

```
# ./configure

Configuring Sudo version 1.6.6

checking whether to lecture users the first time they run sudo... yes
```

NOTE: System will scroll compiler program

2. Install the programs

(Type ‘make install’ to install the programs and any data files and documentation.)

```
# make install
```

NOTE: System will compile program

3. Clean up the temp program files. You can remove the program binaries and object files from the source code directory by typing `make clean'

```
# make clean

    rm -f *.o sudo visudo testsudoers core sudo.core visudo.core \
```

4. Edit the /etc/sudoers files by command visudo
Insert user accounts as follows. (Highlighted)
username!!!!
oracle

```
# visudo

# sudoers file.
#
# This file MUST be edited with the 'visudo' command as root.
#
# See the sudoers man page for the details on how to write a sudoers
file.
#

# Host alias specification

# User alias specification

# Cmnd alias specification

# Defaults specification

# User privilege specification
root    ALL=ALL
oracle   ALL=ALL
username!!!! ALL=ALL
```

```
# Uncomment to allow people in group wheel to run all commands
# %wheel        ALL=(ALL)       ALL
# Same thing without a password
# %wheel        ALL=(ALL)       NOPASSWD: ALL
username!!!!    ALL=(ALL)  NOPASSWD: ALL
# Samples
# %users  ALL=/sbin/mount /cdrom,/sbin/umount /cdrom
# %users  localhost=/sbin/shutdown -h now
sudoers: END
```

GOV LOCATION STATELIDATION

We need to verify the file permissions and verify by logging in and doing the sudo command.

5. Verify Permissions

(This will verify read only permission and ownership by root.)

```
# ls -l /etc/sudoers

-r--r-----   1 root       root           580 Jun  8 11:15 /etc/sudoers
```

6. Login

Verify login username!!!! can sudo.

```
HP-UX dladb02 B.11.11 U 9000/800 (ta)

login: username!!!!

Password:
```

7. SUDO COMMAND

At the prompt enter the following sudo command.

```
$ sudo -u root -s
```

The root prompt should come to the console.

8. Whoami

Now verify you are root by typing the following command.

```
# whoami
whoami
root
```

9. Syslog logging verification

Lastly, verify this GOV Location States logged to syslog.log

```
# tail /GOV Location Stater/adm/syslog/syslog.log
```

```
Jun  8 11:42:19 dladb02 sudo: username!!!! : TTY=pts/ta ;
PWD=/home/username!!!! ; USER=
root ; COMMAND=/usr/bin/sh
```

END OF SUDO DOCUMENT

15.25 Sendmail

The following procedures ensures Sendmail is installed correctly and is secure.

1. Sendmail is downloaded in tar format. Untar the package.

```
# tar –xvf sendmail.8.12.9.tar
x sendmail-8.12.9, 0 bytes, 0 tape blocks
x sendmail-8.12.9/Makefile, 966 bytes, 2 tape blocks
etc………………..
```

2. Set security settings on config files and mail queue.

```
 #chmod go-w / /etc /etc/mail /usr /GOV Location Stater /GOV Location Stater/spool /GOV Location Stater/spool/mqueue
 #chown root / /etc /etc/mail /usr /GOV Location Stater /GOV Location Stater/spool /GOV Location Stater/spool/mqueue
```

3. Set your PATH to compile.

```
# PATH=/usr/sbin:/usr/bin:/usr/ccs/bin:/usr/local/bin:/usr/lib
```

4. export your PATH

```
#export PATH
```

5. Change to sendmail dir.

```
 # cd /h/PUBLIC/sendmail-8*
```

Verify your files below

6. # ls

```
Build        Makefile       contrib     libmilter   mailstats   sendmail
FAQ          PGPKEYS        devtools    libsm       makemap     smrsh
INSTALL      README         doc         libsmdb     obj         test
KNOWNBUGS    RELEASE_NOTES  editmap     libsmutil   praliases   GOV
Location Statecation
LICENSE      cf             include     mail.local  rmail
```

7. # sh Build

```
Making all in:
Etc……………………………………………………
```

8 change directory to cf directory

```
# cd cf/cf
```

9. Copy sendmail mc files to mail directory

```
 # cp generic-hpux.mc  sendmail.mc
```

10. Make the config files

```
# sh Build sendmail.cf
etc…..
```

11. Install files

```
#sh Build install-cf
```

12. cd to sendmail dir

```
#cd ../../
```

13. Build sendmail again

```
# sh Build install
Making all in: etc……..
```

14. Add smmsp group

```
# groupadd -g 25 smmsp
UX: groupadd: GOV LOCATION STATERNING: gid 25 is reserved.
```

15. Verify group

```
#cat /etc/group | grep smmsp
smmsp::25:
```

16. Add smmsp user account

```
 # useradd -u 25 -c "Sendmail" -g 25 –d /h/PUBLIC/smmsp smmsp
UX: useradd: GOV LOCATION STATERNING: uid 25 is reserved.
```

Verify passwd. file

17. # cat /etc/passwd | grep smmsp

```
smmsp:x:25:25:Sendmail:/home/smmsp:/bin/sh
```

18. cd sendmail directory

```
#cd /h/PUBLIC/send*/sendmail
```

17. Start Sendmail

```
# /usr/lib/sendmail -v -bi
/etc/mail/aliases: 3 aliases, longest 10 bytes, 52 bytes total
```

END OF SENDMAIL INSTALL

15.26 Xhost

####INSERT xhost info

15.27 Files not related to

The Servers are for the application and supporting softGOV Location Statere. The servers are not a document repository for personal files of any type. The SA will check all files on the servers and remove files from the servers not authorized for use by . Examples of the types of files not allowed include:

- *.mpg (movie files)
- *.bmp (graphic files not related to Oracle 9i RAC)
- *.jpg (not related to the Application, OEM, or Oracle 9i RAC)

Games of any type (any *.exe or *.com files)
personal web pages or web pages not approved by CM Reston
geoclock (and other applications not approved by CM Reston)

The SA will check the entire system for old tar files on the system. These would include old patches to the secure copy and secure shell, tk8.0, web application, database and datafeed patches, etc.

If the SA is not running the Security Readiness and Review (SRR) on the server, they will move the results of the last SRR to root's home directory and remove the entire SRR directory and files.

There will be no copies of the following list except for where the system puts the files and directories. Backups of the listed files and directories should be on tape.

/etc/init.d
/etc/rc0.d
/etc/rc1.d
/etc/rc2.d
/etc/rc3.d
/etc/rc4.d
/etc/rc5.d
/etc/rcS.d
/etc/mail

Multiple copies of security related files are prohibited. The SA will search for and remove any copies of security related files. An example is the scp command. There will only be one copy located in the /usr/local/bin directory. Other files include:

/usr/local/bin/ssh
/usr/local/bin/scp
/usr/local/sbin/sshd

15.28 SoftGOV Location Statere Versions (swlist –l bundle)

Logging
### INSERT swlist –l bundle

15.29 Logical Volume Manager & MirrorDisk/UX Configuration

vgcfgbackup
vgcfgrestore
Ignite

16 VERITAS Netbackup Overview

Veritas is the Backup and Restore utilized at .

We need to determine what level of involvement we will hCollaboratione.

16.1 Basic Commands for VERITAS NETBACKUP

Veritas commands are broken into 3 categories.

1. Netbackup utilities
/usr/openv/netbackup/bin
/usr/openv/netbackup/bin/admincmd

2. Media Manager utilities
/usr/openv/volmgr/bin

3. Goodies (scripts that are not supported)
/usr/openv/netbackup/bin/goodies
/usr/openv/volmgr/bin/goodies

Optional tools can be downloaded from Veritas.com such as “netbackup.tools.tar and put into the /usr/openv/local/bin directory.

```
autocheckdrives.sh  checkdrives.sh     frozen.sh          monitorjb
autosched.pl        checkdups          gen_excludes       nbimport.sh
backupdb.sh         clam               inactive_classes   rsh.sh
bpGOV Location Stateult.bcv.sh      duplicate.sh       killGOV Location Stateult.sh
bpGOV Location Stateult.copy.sh     epoch.pl           list
bpGOV Location Stateult.sh          fixdrives.sh       makedbtape.sh
```

COMMAND AND USEFUL INFO

Administrative interf.

To get to the administrative interf.

```
#bpadm

        NetBackup Server:  dlaas11


        NetBackup Administration
        ------------------------
        s)  Storage Unit Management...
        t)  Storage Unit Group Management...
        p)  Policy Management...
        g)  Global Configuration...
        r)  Reports...
        m)  Manual Backups...
        x)  Special Actions...
        u)  User Backup/Restore...
        e)  Media Management...
        h)  Help
        q)  Quit

        ENTER CHOICE:
```

To bring up the JCollaborationa administrative interf.

```
#jnbSA &
```

To show listing of active Netbackup Processes.

```
# bpps -a
NB Processes
------------
   root   505     1  0   Nov 05 ?       0:00 /usr/openv/netbackup/bin/bprd
   root   541     1  0   Nov 05 ?       0:03 /usr/openv/netbackup/bin/bpdbm
   root 19281   505  0 20:02:16 ?       0:00 /usr/openv/netbackup/bin/bpsched -ppid 505
   root 19332     1  0 20:02:24 ?       0:03 bpbrm -backup -mt 2 -to 0 -S dlaas11 -c dlaas11 -hostname
dlaas11 -ru root -cl
   root 22042   541  0 23:22:24 ?       0:00 /usr/openv/netbackup/bin/bpdbm
   root 19891 19884  0 20:16:51 ?       0:14 bptm -w -c dlaas11 -den 15 -rt 8 -rn 0 -stunit dlaas11-dlt2-
robot-tld-0 -cl GOV Location Statel
   root 19296     1  0 20:02:18 ?       0:03 /usr/openv/netbackup/bin/bpsched -mainempty
   root 22027   541  0 23:22:22 ?       0:00 /usr/openv/netbackup/bin/bpdbm
   root 19322 19296  0 20:02:22 ?       0:00 /usr/openv/netbackup/bin/bpsched -mainempty
   root 19351 19332  0 20:02:24 ?       0:24 bptm -w -c dlaas11 -den 15 -rt 8 -rn 0 -stunit dlaas11-dlt2-
robot-tld-0 -cl GOV Location Statel
   root 19349     1  1 20:02:24 ?       1:10 bpbkar -r 1129032 -ru root -dt 0 -to 0 -clnt dlaas11 -class
Dlaas11_daily -sche
   root 19890     1  0 20:16:51 ?       3:58 bpbkar -r 1129032 -ru root -dt 0 -to 0 -clnt dlaas11 -class
Dlaas11_daily -sche
   root 19877 19296  0 20:16:48 ?       0:00 /usr/openv/netbackup/bin/bpsched -mainempty
   root 19884     1  0 20:16:50 ?       0:00 bpbrm -backup -mt 2 -to 0 -S dlaas11 -c dlaas11 -hostname
dlaas11 -ru root -cl
   root   543   541  0   Nov 05 ?       0:01 /usr/openv/netbackup/bin/bpjobd


MM Processes
------------
   root   497     1  0   Nov 05 ?       0:00 /usr/openv/volmgr/bin/ltid
   root   542   497  0   Nov 05 ?       0:00 tldd
   root   503     1  0   Nov 05 ?       0:00 vmd
   root   545   497  0   Nov 05 ?       0:00 Collaborationrd
   root   548     1  0   Nov 05 ?       0:00 tldcd
```

Bpmedialist will list show a listing of active allocated media.

```
# bpmedialist
Server Host = dlaas11

 id    rl  images   allocated        last updated      density  kbytes restores
           vimages   expiration       last read       <------- STATUS ------->
--------------------------------------------------------------------------------
EKL079   0     82   10/24/2003 19:01  11/03/2003 21:43    dlt2  109148917       2
               42   11/10/2003 21:43  11/04/2003 20:01
```

```
VK363S   0    238   10/24/2003 18:13  11/07/2003 20:02    dlt2  232605779      0
             84   11/14/2003 20:02  10/29/2003 17:55

VK364S   0     88   11/04/2003 20:02  11/07/2003 20:16    dlt2  92162748      0
             88   11/14/2003 20:16       N/A
```

bpclimagelist will show a listing of images that hCollaboratione not expired.

```
# bpclimagelist
Backed Up          Expires       Files     KB     C   Sched Type   Policy
----------------  ---------- -------- ---------  -  ------------ ------------
11/07/2003 20:08  11/14/2003    44446   1561292  N  Full Backup  Dlaas11_daily
11/07/2003 20:08  11/14/2003        6     40993  N  Full Backup  Dlaas11_daily
11/07/2003 20:07  11/14/2003        6     40993  N  Full Backup  Dlaas11_daily
11/07/2003 20:06  11/14/2003     5442    102313  N  Full Backup  Dlaas11_daily
11/07/2003 20:02  11/14/2003        3        33  N  Full Backup  Dlaas11_daily
11/06/2003 20:23  11/13/2003        6        36  N  Incr Backup  Dlaas11_daily
11/06/2003 20:22  11/13/2003        6        34  N  Incr Backup  Dlaas11_daily
11/06/2003 20:22  11/13/2003        6        35  N  Incr Backup  Dlaas11_daily
11/06/2003 20:21  11/13/2003      463    136855  N  Incr Backup  Dlaas11_daily
11/06/2003 20:20  11/13/2003        4        33  N  Incr Backup  Dlaas11_daily
11/06/2003 20:19  11/13/2003        8    118914  N  Incr Backup  Dlaas11_daily
11/06/2003 20:19  11/13/2003        3        33  N  Incr Backup  Dlaas11_daily
11/06/2003 20:19  11/13/2003        6        33  N  Incr Backup  Dlaas11_daily
```

INDEXING(For indexing number of directory levels 0 - 9. This has pros and cons for both restores and backups.)

```
# ./index_clients

The clients are already indexed with a default index level of 9.

Do you GOV Location Statent to recreate the index files for all the clients? (y/n) [n] n
```

16.2 Backup

Netbackup is used to either backup or to archive files.

1. Backup will write data to tape or disk and will not delete the files from the filesystem.
2. Archive will write data to tape or disk and WILL delete the files from the filesystem.

There are three levels of backups in Netbackup.

1. Full Backup – Does a zero level backup of the file system.
2. Incremental
   *Cumalitive – Backup from last full backup
   *Differential – Backup from last Full or Incremental backup
3. User Backup – User initiated backup

For further info refer to the “Netbackup Systems Administrators Gu for Unix or Netbackup Users Gu for Unix

16.3 Restore

For further info refer to the “Netbackup Systems Administrators Gu for Unix or Netbackup Users Gu for Unix

APPENDIX A - Points of Contact List

Project Office					
Name	**Address**	**Phone**	**E-Mail**	**Area**	**Command**

######OBTAIN CONTACT INFO

APPENDIX B - Status of Datafeeds for GOV PROGRAM Implementation

### DETERMINE STATUS AND INSERT DATAFEEDS FOR IMPLEMENTATION

APPENDIX C - GLOSSARY OF TERMS

Clusters = Two or more computers in a networked configuration that will allow continued application access in spite of a hardGOV Location Statere or softGOV Location Statere failure.

Exporting = Sending data acquired within into a file format to be used in another application.

Failover = In HA Clusters when the (Active) Primary node failsover to the Adoptive node

Failback = In HA Clusters when the Active (Adoptive node) goes back to Primary node

Host IP Address = Host Internet Protocol Address. It is the address of the database. Internet Protocol (IP) is a packet-switching protocol that provs a common layer over dissimilar connectionless networks. Every computer connected to the Internet has its own unique IP Address. The Development Team provs the Host IP Address to you.

Importing = Bringing in data from an external source.

= GOV PROGRAM.

Node = Host in a HA cluster. In SericeGuard there Primary, Adoptive and Active nodes.

Package = Application or group of applications in HA Cluster

Query = A method of using Structured Query Language (SQL) to retrieve needed information from the database.

RAC REAL APPLICATION CLUSTERS = Oracle specific database instance clustering

SQL = A structured query language that permits access to relational database management systems.

APPENDIX D - User Account Application

The User Account Application should be used as the basis for creating new accounts (for Unix, SQL, or Web). Any local command-required paperwork should be included with this form to assist in the processing.

The form can be updated to include local addresses and server names. Electronic copies of this form can be obtained from the GOV CONTRACTOR/PRIME CONTRACTOR Help Desk.

#### will need to define the requirements for user authorization, Below is an example form that could be used/

USER ACCOUNT APPLICATION

####INSERT LOGO

The following form is to be distributed to sites that will need access to systems.

EXAMPLE USER ACCESS FORM

Name of User: ____

Organization: ____

Address: ____
____

Access Requirement (Please circle): **Web** **Unclassified** **Classified**

Access duration: **Beginning Date**____________ **End Date:** _____________

E-mail Address: **Unclassified:** _________________ **Classified:** ___________________

Telephone: __________________ **FAX:** ________________

Security Clearance: _______________ **Security Officer:** __________________________

Security Officer's Telephone: __________________ **FAX:** ________________

Approving Official (Need to know verification):

Name:________________ **Date Approved:** ___________ **Phone:**______________

Approving Official:

Name:________________ **Date Approved:** __________ **Phone:**_______________

OFFICE USE

Account Information:

Servers: _________ **UID:** ______ **GID:** ______ **Login:** _______ **Temp Password:** _______
_________ **UID:** ______ **GID:** ______ **Login:** _______ **Temp Password:** _______
_________ **UID:** ______ **GID:** ______ **Login:** _______ **Temp Password:** _______
_________ **UID:** ______ **GID:** ______ **Login:** _______

Icon Established (Circle): **yes** **no** **N/A**
Permissions (Circle all that apply): **Connect** **Resource** **DBA**

APPENDIX E – IGNITE/UX CONFIGURATION SCRIPT

#####INSERT IGNITE/UX SCRIPT HERE

APPENDIX F – Unix Shell Backup Script

###INSERT Backup SCRIPT HERE

APPENDIX G – SUPPORT INFORMATION

REMOVED FOR CONFIDIATIALITY

HPUX
Oracle
Veritas

APPENDIX H - File and Directory Permissions

####INSERT FILES LIST HERE

END OF DOCUMENT