OLS Evaluated Configuration for
Oracle Database 10*g* Release 1 (10.1.0)

November 2005

Security Evaluations
Oracle Corporation
500 Oracle Parkway
Redwood Shores, CA 94065

OLS Evaluated Configuration for Oracle Database 10*g*
Release 1 (10.1.0)

November 2005

Author: Saad Syed

Contributors: Peter Goatly, Shaun Lee

This document is based on the equivalent document for OLS for Oracle9i Release 2, Issue 1.0 [OLSECD_10] used in the last Common Criteria Evaluation of Oracle9i with OLS. The contributions of the many authors of the precursors to this document are acknowledged. Change bars indicate changes made relative to [OLSECD_10].

Contents

Contents

CHAPTER

1 Introduction

The Target of Evaluation (TOE) is the Oracle Database 10*g* Release 1 (10.1.0.4.0) Object-Relational Database Management System (O-RDBMS) with Oracle Label Security.

The TOE is hosted on the Red Hat Linux AS (Version 3) operating system platform.

This *OLS Evaluated Configuration for Oracle Database 10g* document explains the manner in which the TOE must be configured along with the host operating system and network services so as to provide the security functionality and assurance as required under the Common Criteria for Information Technology Security Evaluation [CC].

The assumptions and procedures stated in the document are all (by and large) intended to remove potential vulnerabilities or attack paths from the TOE in its environment. They do not have any impact on the correct implementation of the SFs.

The Evaluation Assurance Level for the TOE is EAL4 augmented with ALC_FLR.3. The Protection Profile used for the evaluation of the TOE is the Database Management System Protection Profile [DBPP]. The Security Target used for the evaluation of the TOE is [ST].

1.1 Intended Audience

The intended audience for this document includes evaluators of the TOE, system integrators who will be integrating the TOE into systems, and accreditors of the systems into which the TOE has been integrated.

1.2 Organization

This document is composed of the following sections:

Chapter 1 contains the introduction to the document;

Chapter 2 describes the physical environment of the TOE and the network services required to support the TOE;

Chapter 3	describes the host operating system, network services, and client application configurations required to support the TOE;
Chapter 4	describes the configuration of the TOE, and all TOE-related network services and applications;
Chapter 5	contains a step by step guide to installation of the TOE in its evaluated configuration;
Annex A	details the password management controls that must be implemented in all user profiles;
Annex B	lists the software components installed as per Section 5.2;
Annex C	lists the Linux packages installed in the evaluated configuration and
Annex D	lists the references that are used in this document.

1.3 Format

Assertions for the physical, host, and Oracle configurations are given identifiers to the left of each evaluation configuration requirement in bold Helvetica font, e.g. **[A-1]**. The names of the identifiers have not changed from one release to the next even when some assertions have been removed because they are no longer applicable.

References to sections of documents listed in Annex E are in the format [*document, section*].

Mandatory evaluation configuration requirements use the words “must” and/or “shall” in each assertion.

Strongly recommended evaluation configuration requirements use the words “should” in each assertion.

CHAPTER

2 Physical Configuration

This chapter describes the physical and procedural requirements for maintaining the security of the TOE.

2.1 Physical Environmental Assumptions

[A-1] The processing resources of the TOE shall be located within controlled access facilities which will prevent unauthorized physical access to the TOE by unprivileged users. Only authorised DBA or operator users (i.e. users who are allowed corresponding SYSDBA or SYSOPER access rights within the database) shall have physical access to the server machines.

[A-2] The processing resources of the underlying operating system required to support the TOE shall be located within controlled access facilities which will prevent unauthorised physical access.

[A-3] The processing resources of the network services required to support the TOE shall be located within controlled access facilities which will prevent unauthorised physical access.

[A-4] The media on which authentication data for the underlying operating system data resides shall not be physically removable from the underlying operating system by unauthorised users.

[A-5] The media on which the TOE audit data resides shall not be physically removable from the underlying operating system by unauthorised users.

[A-6] Any on-line and/or off-line storage media on which security relevant data resides shall be located within controlled access facilities which will prevent unauthorised physical access.

2.2 Supporting Procedures

Procedures for the administration of TOE security shall be established based on the contents of this document, the Security Target [ST], any site security policy that may be in force, and [ECGR], [SRN] and [ECGS]. In particular procedures shall be estab-

lished such that:

- users must not disclose their operating system passwords to other individuals;
- operating system or database passwords generated by the system administrator shall be distributed in a secure manner;
- procedures and/or mechanisms shall assure that, after system failure or other discontinuity, recovery without a protection (i.e. security) compromise is obtained;
- the on-line and off-line storage media on which security related data (such as operating system backups, database backups and transaction logs, and audit trails) are held shall be properly stored and maintained, and routinely checked to ensure the integrity and availability of the security related data;
- the media on which database-related files (including database files, export files, redo log files, control files, trace files, and dump files) have been stored shall be purged prior to being re-used for any non-database purpose;
- the predefined normal users SYS, SYSTEM, LBACSYS and users who connect as SYSDBA or SYSOPER are highly trusted users, who are required by the architecture of the TOE to be able to perform privileged database operations for which the TOE records only limited information. It is assumed that appropriate personnel and procedural measures (such as procedural two-person control) will be provided to ensure that operations performed under these trusted user accounts conform to the system security policy. (Note that the TOE records accounting information for operations performed by SYS, DBA and OPER to the OS audit trail, but only if the `audit_sys_operations` initialization parameter is set to TRUE).

  For more routine administration tasks it is recommended that alternative, less privileged, database user accounts are configured and used to perform a more restricted set of privileged database operations.
- a user who grants the REFERENCES privilege on one or more columns of a table shall understand the possible interactions between database referential integrity controls and access controls. Specifically, a referential constraint has the following implications:
  - if the referential constraint specifies DELETE RESTRICT then a user will not be able to delete referenced parent rows even though the user has DELETE access on the parent table;
  - if the referential constraint specifies SET TO NULL or SET TO DEFAULT then when a parent row is deleted from the parent table the corresponding child row(s) will be updated regardless of whether the deleting user has UPDATE access on that child table.
  - if the referential constraint specifies DELETE CASCADE then when a parent row is deleted from the parent table the corresponding child row(s) will be deleted from the child table regardless of whether the deleting user has DELETE access on that child table.
- Administrators shall understand the limitations of resource limits. The TOE can control certain resources such as user sessions and connect time directly, but 'system' resources such as CPU time and logical reads can only be controlled in relation to statements that the database has to process (i.e. SQL and PL/SQL statements). For example, the O-RDBMS can run Java code internally, but as this is a separate server mechanism the program code itself is not subject to resource

limits. However any database calls (SQL) made from the Java code are sent from the Java Engine to the database SQL engine, then processed in the normal way and are subject to all applicable resource limits.

- Administrators, through the use of password limits in profiles, shall ensure that password controls for all users (including trusted administrative users) are strong enough to satisfy the TOE's CC Strength of Function rating of SOF-*high*.
- Administrators should be aware, when creating new profiles or when changing the default profile, of the factors influencing the strength of user passwords. **[DB.IA-18]** ensures that certain limits are set in every profile (although it does offer a choice to administrators), however the other password controls available can both strengthen and weaken the TOE's overall password mechanism strength. In general, any further elaboration of the complexity check function (beyond that suggested in this document) will **weaken** the strength of passwords since it would narrow the choice available. The other controls are however generally strengthening measures. A password_lock_time in conjunction with failed_login_attempts will delay any password-guessing attacks (although a lockout time of at least 1 minute, and a failed logins count of <10 is recommended). Setting a password_life_time (in conjunction with password_grace_time) will limit the opportunity of an attacker to guess a particular password. Also, using the password_reuse_time limit will enforce the use of different passwords, again limiting the opportunity for a particular password to be guessed. To prevent the same password being supplied at the end of a password life-time period, administrators should set password_reuse_time greater than password_life_time.
  Note that "password_reuse_time" should be interpreted as the time between the last successful user password change to a given value and the next attempt to change the user's password to that same value.
- Administrators shall not open databases in read-only mode. The read-only database open feature provides the ability for users to query an open database without the potential for on-line data contents modification. This mode of operation deactivates some security features including password changing, account lockout, and database auditing.

This Page Intentionally Blank

CHAPTER

3 Host Configuration

This chapter describes the configuration requirements for the Red Hat Linux server platform, the network services and the client platforms. It also covers the use of operating system facilities to protect the TOE.

3.1 Red Hat Enterprise Linux Operating System

The TOE was evaluated and tested on a IBM xSeries 335 Xeon server connected to a Compaq Deskpro EN Pentium 3 client. These machines were connected by a Local Area Network (LAN).

The TOE was evaluated and tested on Red Hat Enterprise Linux AS (Version 3) which has met Common Criteria security requirements for assurance level EAL 3+.

[RH-3] Red Hat Linux shall be installed and operated in a manner described in [ORHEL], [ECGR], Chapter 3 and Annex D of this document.

[RH-4] The ext3 filesystem shall be used on all host machines supporting the TOE.

[RH-5] The operating system administrator shall ensure that only designated users are able to perform administrative tasks in the operating system.

In addition the only local operating system user accounts on the server shall be those for the DBA administrators and OS administrators.

3.1.1 Identification and Authentication

[RH.IA-6] No non-administrative users (existing or newly created) shall belong to the administrative groups on either the host machine on which the TOE is installed, or on their local (client) machines from which they will connect to the TOE.

See **[RH-5]** for guidance about such administrative groups.

[RH.IA-8] All normal operating system users shall have a non-administrative primary group set, such as `USERS` or `ORA_USERS`.

3.1.2 Protection of Resources

[RH.PR-1] The operating system shall protect all of the installed TOE-related files and directories

by means of its Discretionary Access Control mechanisms to ensure that they are accessible to authorised users only.

Oracle Universal Installer, Database Configuration Assistant and Database Upgrade Assistant set file permissions when Oracle software is installed, so no further action is required.

[SG, 2-6: Restrict Operating System Access] describes best practice in restricting operating system access.

[RH.PR-4] To maintain the integrity of the audit timestamp, only operating system administrators shall have access to the operating system clock configuration. All other users shall have no access permissions for the operating system clock configuration.

3.1.3 Accounting and Auditing

[RH.AA-1] The operating system shall protect operating system audit trails or any other audit trails (e.g. audit log files) used by the O-RDBMS against unauthorized modification and deletion by means of its Discretionary Access Control mechanisms.

[RH.AA-2] The directory containing the TOE-generated audit log files shall have permissions set for only the local TOE administrator operating group, and no access for all other users. Note: this is located by default in the *$ORACLE_HOME/rdbms/audit* directory.

[RH.AA-3] The operating system administrator shall include procedures that support the archiving of operating system audit trails and audit log files prior to audit trail or disk space exhaustion.

3.2 Network Services

[OS.NS-3] In a distributed environment, the underlying network services shall be based on the available secure communication protocols which ensure the authenticity of the operating system users.

[OS.NS-4] Only administrative users shall be able to modify the network services configuration parameters.

3.3 Client Applications

[OS.CA-1] No applications shall be permitted to run on any client or server machines which access the network, unless they have been shown not to compromise the TOE's security objectives stated in the [DBPP] and the [ST].

CHAPTER

4 Oracle Configuration

The TOE consists of software only. The TOE contains no hardware or firmware components and there are no hardware or firmware dependencies which affect the evaluation.

The TOE shall be installed, configured, and maintained in accordance with this document and with the instructions provided in [INST_LINUX_10*g*] and [ORHEL].

4.1 O-RDBMS Server

4.1.1 Identification and Authentication

In the evaluated configuration for the Red Hat Linux platform only the O-RDBMS mode of Identification and Authentication is supported. OS Authentication should not be enabled on any of these platforms.

[DB.IA-1] For the Red Hat Linux platform the TOE shall be configured to use O-RDBMS I&A for all users connecting to the TOE, i.e. all database users must have a *database password.*

[DB.IA-2] Administrators whocreate normal users within the O-RDBMS shall create appropriately privileged accounts for those users in the operating system as well. See **[RH.IA-8]**, **[SS.IA-8]** and **[SL.IA-8]** for details.

[DB.IA-3] Database administrators shall set the initialization parameter as follows:

```
o7_dictionary_accessibility = FALSE
```

This ensures that if you need to access objects in the SYS schema, explicit object privilege must be granted to you. System privileges that allow access to objects in "any schema" do not allow access to objects in SYS schema.

[DB.IA-4] After creating and setting up a database, all database user accounts must be configured as per **[DB.IA-1]**. All pre-defined accounts (such as SYS, MDSYS, SYSTEM etc.) and any demonstration accounts (such as SCOTT) created during installation should have their passwords changed.

[DB.IA-7] Database administrators shall set the initialization parameter as follows:

```
sql92_security = TRUE
```

This ensures that the user must have SELECT privilege on a table when executing an UPDATE or DELETE statement that references table column values in a WHERE or SET clause.

[DB.IA-11] Normal database users may belong to one or more of the following operating system local groups.

```
ora_user
ora_<sid>_user
```

This step is discretionary, it may help distinguish database users from other users, however it is not necessary for users to belong to this user group in order to connect to the database.

[DB.IA-14] To connect to the O-RDBMS as a privileged database user such as a database administrator, the following parameter shall be set in the appropriate initialization file:

```
remote_login_passwordfile = EXCLUSIVE
```

This allows two types of privileged connection. Privileged connections (i.e. AS SYSDBA, AS SYSOPER) are permitted either by having an entry in the password file (having been granted the appropriate permissions in the database), or by membership of an OS group (having been granted membership by an OS administrator).

[DB.IA-15] Database administrators who are required to use the CONNECT / AS SYSOPER syntax to connect to an O-RDBMS shall belong to one or more of the following operating system local group:

```
dba
```

[DB.IA-16] Database administrators who are required to use the CONNECT / AS SYSDBA syntax to connect to an O-RDBMS shall belong to one or more of the following operating system local group:

```
dba
```

[DB.IA-18] After creating and setting up a database, the default profile must be changed as described in Annex A of this document. Annex A provides a choice of two profiles, which implement password limits that enable the TOE to satisfy its CC Strength of Function claim. Database administrators must also employ this change to all new profiles created, to ensure that all users (including administrative users) are subject to strong password controls at all times. The guidance in section 2.2 should be followed when modifying or creating profiles.

[DB.IA-19] Administrators wishing to limit password reuse (for example to prevent the same password being supplied at the end of a password life-time period), should use the profile setting password_reuse_time, perhaps in conjunction with password_life_time and password_grace_time (with password_reuse_time being set greater than password_life_time). The profile setting password_reuse_max should not be used.

[DB.IA-20] In the evaluated configuration roles shall not be protected by an associated password.

4.1.2 Accounting and Auditing

[DB.AA-2] In the evaluated configuration for a specific O-RDBMS, the `audit_trail` parameter in the appropriate initialization parameter file for that O-RDBMS shall be assigned in one of the following two ways:

```
audit_trail = OS
```

```
audit_trail = DB
```

[DB.AA-3] When OLS has been installed, the database audit trail is a SYSTEM-owned table, SYSTEM.AUD$. Only users connected as AS SYSDBA or SYSTEM can directly read and write all rows in SYSTEM.AUD$ (provided that **[DB.AC-10]** has been complied with).

[DB.AA-5] Database administrators shall create database audit trail views for all other appropriately privileged O-RDBMS users to be able to read and analyse database audit trail data.

Pre-defined database audit trail views are automatically created during the installation and creation of the database.

Only highly trusted users shall have the privilege which allows them to:

- set or alter the audit trail configuration for the database;
- alter or delete any audit record in the database audit trail.

[DB.AA-6] Database administrators shall perform regular archiving of database and operating system audit trails before audit trail exhaustion to ensure sufficient free space for continued auditing operations. See Section 3.1.3 or 3.2.3 for details.

[DB.AA-7] Database administrators shall ensure that session auditing is enabled at all times by issuing the statement

```
audit session;
```

By enabling session auditing at all times, all user sessions are recorded with their sessionid and method of authentication. This information can then be used to identify whether actions in a particular session were undertaken by a proxy user.

[DB.AA-9] Database administrators shall ensure that changes to the database audit trail are audited, by issuing the statement

```
audit insert, update, delete
on system.aud$
by access;
```

[DB.AA-10] Since fine-grained auditing is supported only with cost-based optimization, database administrators shall ensure that the cost-based optimization mode is used when using fine-grained auditing. This can be achieved by setting the `optimization_mode` parameter in the appropriate initialization parameter file in one of the following ways:

```
optimizer_mode = first_rows_n  (where n = 1, 10, 100 or 1000), or
optimizer_mode = all_rows
```

4.1.3 Availability and Reliability

[DB.AR-1] Only privileged O-RDBMS users such as database administrators shall be permitted to perform privileged O-RDBMS operations such as backup and recovery, and enforce tablespace quotas and resource profiles.

[DB.AR-2] **[DB.AR-1]** should be accomplished by ensuring that only privileged O-RDBMS users have the necessary administrative system privileges to perform these types of operations.

[DB.AR-3] Administrative system privileges shall not be granted to normal O-RDBMS users directly or through the use of database roles. See Section 4.1.5 for details.

For example, a normal O-RDBMS user must not be granted the `ALTER PROFILE` system privilege either directly or through a database role.

[DB.AR-4] Each user of the TOE must be configured with appropriate tablespace quotas that are

- sufficiently permissive to allow the user to perform the operations for which the user has access rights;
- sufficiently restrictive that the user cannot abuse the access rights and thereby waste or monopolise resources.

4.1.4 DAC Access Controls

[DB.AC-5] If the UTL_FILE PL/SQL package is used to provide database access to host OS files the configuration parameter `UTL_FILE_DIR` must not be set to "*", but to explicit values so as to protect against overriding the operating system DAC mechanisms.

[DB.AC-6] Each database link must be defined such that users who refer to the link are connected to an identically named normal user account in the secondary or remote database, that is the database link must be defined without reference to a single normal user account to which all users referencing the link would otherwise be connected.

[DB.AC-7] The EXECUTE privilege on the DBMS_JOB, UTL_SMTP, UTL_TCP, UTL_HTTP, UTL_FILE, DBMS_RANDOM PL/SQL packages is granted to PUBLIC by default. This should be revoked by executing the following SQL statements from an administrative connection to the database:

```
revoke execute on <package_name> from public;
```

[DB.AC-8] The EXECUTE privilege on the SA_COMPONENTS, SA_USER_ADMIN, SA_LABEL_ADMIN, SA_POLICY_ADMIN and SA_AUDIT_ADMIN OLS packages shall only be granted to OLS policy administrators.

[DB.AC-9] The EXECUTE privilege on the SA_SYSDBA OLS package shall only be granted to database administrators.

[DB.AC-10] Normal users shall not be granted access to objects in the SYSTEM or LBACSYS schemas.

4.1.5 Security Administration and Management

In the evaluated configuration, the TOE supports and implements Security Administration and Management by the use of over ninety distinct and separately managed object and system privileges. When OLS is installed, OLS policy privileges are also available.

System privileges which are administrative in nature such as those which allow database-wide object, role, user, privilege, and profile manipulation shall not be granted to normal O-RDBMS users either directly or through database roles.

[DB.SAM-1] Only highly trusted O-RDBMS users and database administrators should be allowed to possess system privileges which are administrative in nature.

Examples of such privileges are the `ALTER PROFILE` and `ALTER USER` system privileges which can be used to alter any user profile, or any user in the O-RDBMS.

The latter gives full access to other users' accounts, either through altering their passwords or through the ability to proxy as them.

[DB.SAM-2] Object privileges and other system privileges (which are non-administrative in nature) are required by normal O-RDBMS users to perform their tasks under the *Principle of Least Privilege.*

The privileges described above should be grouped together into database roles and granted to normal O-RDBMS users.

An example of these types of privileges is the `CREATE TABLE` privilege which by default allows O-RDBMS users to create and modify tables within their own schema, but not in any other user schema.

[DB.SAM-3] The system privileges of `SYSDBA` and `SYSOPER` shall not be granted to any normal O-RDBMS user, including the user `SYSTEM`.

Database administrators are authenticated as described by DB.IA-14 above. Only database administrators should be granted these system privileges, or given membership of the OS groups described in DB.IA-15 and DB.IA-16.

[DB.SAM-5] The `CREATE LIBRARY` and `CREATE ANY LIBRARY` system privileges shall not be granted to any user of the TOE.

This restriction is imposed so as to prevent the use of libraries which would enable callouts to external C programs which could be misused against the TOE's security features.

[DB.SAM-6] The `CREATE SNAPSHOT`, `CREATE MATERIALIZED VIEW`, `CREATE ANY SNAPSHOT`, `CREATE ANY MATERIALIZED VIEW`, `ALTER ANY SNAPSHOT` or `ALTER ANY MATERIALIZED VIEW` privileges shall only be assigned to trusted (e.g. DBA) users.

[DB.SAM-7] In the evaluated configuration the use of Java packages is not supported. Database Administrators shall make regular checks to ensure that users do not use Java packages.

[DB.SAM-8] LBAC user authorisations and OLS policy privileges are required by normal O-RDBMS users to perform their tasks under the *Principle of Least Privilege.*

[DB.SAM-9] The OLS FULL policy privilege shall not be granted to normal users of the TOE.

[DB.SAM-10] The OLS PROFILE_ACCESS policy privilege shall not be granted to normal users of the TOE. This is a very powerful privilege, since the user can potentially become a user with FULL privileges.

[DB.SAM-11] When OLS has been installed, the `CREATE TRIGGER` system privilege shall not be granted to any normal user of the TOE. This is because `CREATE TRIGGER` allows a user to set a trigger on one of his tables which can potentially run with FULL privileges if another user accesses that table.

[DB.SAM-12] The roles `CONNECT` and `RESOURCE` shall not be granted to normal users of the TOE. These roles are only provided to maintain compatibility with previous versions of Oracle and may not be provided in future versions of Oracle. Instead, the privileges which make up these roles should individually be granted to users or to a role as needed by the user. See [SG, 10: User Roles (Table 10-1)].

[DB.SAM-13] The EXEMPT ACCESS POLICY system privilege shall only be given to users who have legitimate reasons for by-passing fine-grained security enforcement of VPD or OLS policies.

[DB.SAM-14] Because system privileges are so powerful, administrators must take great care when granting `ANY` system privileges to non-DBA users (such as `UPDATE ANY TABLE`). Such privileges shall only be given to users who have legitimate reasons for their use.

In particular, `CREATE ANY TRIGGER` shall not be granted to non-DBA users. This is because it allows a user to create a trigger on any database table and hence to capture data from any transaction performed on that table.

[DB.SAM-15] [ADG, 15: Database Administration Tasks Before Using Flashback Features] describes how DBAs should set up a database for flashback queries. DBAs should only grant the `FLASHBACK ANY TABLE` privilege or `EXECUTE` on the `DBMS_FLASHBACK` package to trusted users who have legitimate reasons for their use, because this allows such users to access data that existed in the past in tables that they can currently access. This would be a problem if the owner of a table had deleted rows that held sensitive information before granting other users privileges to access the table.

For the same reason, DBAs should refuse requests from normal users to be granted the `FLASHBACK` privilege on a table that they do not own. They should, instead, ask such a user to request the owner of the table to grant them the `FLASHBACK` privilege.

[DB.SAM-16] As described in **[DB.SAM-15]**, DBAs should refuse requests from normal users to be granted the `FLASHBACK` privilege on a table that they do not own. They should, instead, ask such a user to request the owner of the table to grant them the `FLASHBACK` privilege. The owner of a table which is protected by VPD policies should refuse requests from normal users to be granted the `FLASHBACK` privilege on the table unless the administrators for these VPD policies have given their approval. The reason for this is that otherwise there would be a problem if a row in a table protected by a VPD policy has had data in a column updated to make access to the row via the policy more restricted, because a flashback query could allow a user access to the row when the VPD policy should not permit it.

[DB.SAM-17] As described in **[DB.SAM-15]**, DBAs should refuse requests from normal users to be granted the `FLASHBACK` privilege on a table that they do not own. They should, instead, ask such a user to request the owner of the table to grant them the `FLASHBACK` privilege. The owner of a table which is protected by OLS policies should refuse requests from normal users to be granted the `FLASHBACK` privilege on the table unless the administrators for these OLS policies have given their approval. The reason for this is that otherwise there would be a problem if a row in a table protected by an OLS policy has had its label updated to be more restrictive, because a flashback query could allow a user access to the row when his label authorisations should not permit it.

4.1.6 Secure Data Exchange

[DB.SDE-1] Database administrators shall ensure that any system privilege (directly or through the use of roles) required to implement database import and export be only granted to O-RDBMS users who are trusted to perform these operations, and who normally do not have the appropriate privileges for read and write access to such data.

4.1.7 Secure Distributed Processing and Databases

The TOE can be operated in standalone, client/server and server/server configurations. Database links may be used to connect between different O-RDBMS servers over a network. The TOE provides site autonomy which implies that each server participating in a distributed environment is administered independently from other servers in the distributed system.

[DB.SDD-1] Database administrators should implement a site-specific security policy according to

their security requirements.

When distributed databases are employed, OLS Policy administrators should use the same label tags for each database. If this is not possible then users should ensure that they convert labels to character strings upon retrieval (using LABEL_TO_CHAR) and use CHAR_TO_LABEL when storing labels. This ensures that labels are consistent even if the corresponding label tags are different on the remote database.

In a distributed environment, the OLS policy administrator should ensure the same relative ranking of the numeric form of the level component, in order to ensure proper dominance of the labels.

4.1.8 Multi-tier environments

[DB.MT-1] To ensure accountability in multi-tier environments, any middle-tier(s) must pass the original client ID through to the TOE.

4.2 Oracle Network Services

[DB.NS-3] Only operating system or database administrators shall be able to modify the installed network services configuration parameters.

[DB.NS-4] No other user should be permitted to modify any network services configuration parameter in the O-RDBMS network configuration files such as `TNSNAMES.ORA`, `LISTENER.ORA` and `SQLNET.ORA`.

[DB.NS-5] The network services configuration files specified in DB.NS-4 are located in *$ORACLE_HOME*`\NETWORK\ADMIN`. Permissions on this directory should be restricted so that administrative users have full access, but all other operating system users have read-only access.

[DB.NS-7] The parameters in the network configuration files specified in DB.NS-4 shall use a consistent O-RDBMS naming convention; this helps ensure database uniqueness throughout the domain.

This Page Intentionally Blank

CHAPTER

5

Step by Step Guide

This chapter contains a step by step guide to installing the TOE in its evaluated configuration.

Readers unfamiliar with Oracle products should read this section in conjunction with [DAG]. Note that in some cases changes are not effective until the database is restarted or, for membership of an OS user group, until the user has logged out and logged in again.

5.1 Operating System Installation / Configuration

Ensure that the intended physical environment is in accordance with the assumptions **[A-1]** to **[A-6]** listed in section 2.1 of this document.

5.1.1 Installation of Red Hat AS (Version 3)

Install Red Hat AS (Version 3) in accordance with [ORHEL], [ECGR], Chapter 3 and Annex D of this document.

5.2 Oracle Database 10*g* Server Installation / Configuration

5.2.1 Step by Step Installation of Oracle Database 10*g* Release 1 (10.1.0)

This section outlines generic steps needed to duplicate the evaluated configuration of Oracle Database 10*g*. The steps describe an installation that can be used as a guide for the Red Hat Enterprise Linux AS Server platform. Those steps which are essential towards achieving the Evaluated configuration are highlighted in **bold**.

This section should be used in conjunction with the relevant installation manuals and assumes any prior installations of Oracle Database 10*g* O-RDBMS have been subsequently removed. Some screens only appear during the first installation of the Oracle

Database on a system.

Step No.	Action	Result
1	Insert the Oracle Database 10*g*disk. Follow the installation instructions to start Oracle Universal Installer.	Oracle Universal Installer: Welcome window appears.
2	Click Next.	Specify Inventory directory and credentials page opens.
3	Ensure details are correct. Click Next. Execute orainstRoot.sh script and click Continue.	Specify File Locations page opens.
4	Ensure the Oracle Home and full path details are suitable for the installation. Click Next.	Select Installation Type page opens.
5	**Select Custom and click Next.**	Product-Specific Prerequisite checks page opens.
6	Click Next	Available Product Components page opens.
7	**Deselect all components except the following:** **Oracle Database 10*g* 10.1.0.3.0** **Oracle Database 10*g* 10.1.0.3.0** **Sun JDK extensions 9.0.4.0.0** **Enterprise Edition Options 10.1.0.3.0** **Oracle Label Security 10.1.0.3.0** **Oracle Net Services 10.1.0.3.0** **Oracle Net Listener 10.1.0.3.0** **Click Next.**	Privileged Operating System Groups page opens.
8	Ensure groups are suitable. Click Next.	Create Database page opens.
9	Select Yes and click Next.	Summary page opens.
10	**Ensure Summary list of installation components is identical with the Server components listed in Appendix B of this document.**	Lists are indentical.
11	Click Install	Install page opens and installation begins.

Step No.	Action	Result
12	Run root.sh script. Click OK. Click Next.	Oracle Net Configuration Assistant Welcome page opens.
13	Click Next.	Listener Configuration, Listener Name page opens.
14	Select a suitable Listener name and click Next.	Listener Configuration, Select Protocols page opens.
15	Select TCP only and click Next.	Listener Configuration, TCP/IP protocols page opens.
16	Select Use the standard port number of 1521 and click Next.	Listener Configuration, More Listeners? page opens.
17	Select No and click Next.	Listener Configuration Done page opens.
18	Click Next.	Naming Methods Configuration page opens.
19	Select No, I do not want to change the naming methods configured. Click Next.	Oracle Net Configuration Assistant ends.
20	Click Finish.	Database Configuration Assistant: Step 1 of 11: Database Templates page opens.
21	Select Custom Database. Click Next.	Step 2 of 11 : Database Identification page opens.
22	Choose a Global Database Name e.g. ols1.test. Click Next.	Step 3 of 11 : Database Templates page opens.
23	Click Next.	Step 4 of 11 : Management Options page opens.
24	Select suitable passwords. Click Next.	Step 5 of 11 : Storage Options page opens.
25	Select File System. Click Next.	Step 6 of 11 : Database File Locations page opens.
26	Select appropriate location. Click Next.	Step 7 of 11 : Recovery Configuration page opens.

Step No.	Action	Result
27	Deselect Specify Flash Recovery Area. Click Next.	Step 8 of 11 : Database Content page opens.
28	Deselect all components and **select Oracle Label Security**. Click Next.	Step 9 of 11 : Initialization Parameters page opens
29	**Ensure Dedicated Server is selected** and appropriate initialization parameters. Click Next.	Step 10 of 11 : Database Storage page opens.
30	Click Next.	Step 11 of 11 : Creation Options page opens.
31	Select Create Database. Click Finish.	Confirmation Window opens.
32	If details correct click OK.	Database Configuration Assistant creates database.
33	Click Exit	Database Configuration Assistant exits.

5.2.2 Exclusions

This document implicitly excludes certain components by specifying the installation options that comprise the TOE boundary. Additionally, the guidance and configuration steps contained in this document prohibit the use of certain other facilities.

Administrators should also be aware of facilities that should not be used during development of database applications in the evaluated configuration. These are the iFS (internet File System), the OCI internet cache, the KG platform (which implements PL/SQL metadata sharing in applications), the Thin JBDC driver (which provides java applets with a non-OCI interface to the database), the Oracle Intelligent Agent and the new Java RepAPI protocol for snapshots (which is similar to the thin Java client interface).

5.3 Installation of Patch Set for Oracle Database 10*g* (10.1.0.4)

Installation of the Oracle Database 10*g* Patch Set (10.1.0.4) was in accordance with the instructions given in the Oracle Database 10*g* Patch Set Notes [PSN-Linux].

5.4 Installation of Critical Patch Update July 2005

Installation of the Oracle Critical Patch Update July 2005 was in accordance with the instructions given in the Oracle Critical Patch Update July 2005 Release Notes for Oracle Database Server Version 10.1.0.4.0 for both platforms [CPU-Notes].

5.5 Configuration of Oracle Database 10*g* RDBMS

5.5.1 Protection of database files

Protect the database files from unauthorised access as per **[SS.PR-1]**, **[RH.PR-1]** and **[SL.PR-1]** of sections 3.1.2, 3.2.2, and 3.3.2. Network files shall be protected as per **[DB.NS-3]** to **[DB.NS-5]** of section 4.2.

5.5.2 Setting up the Evaluated Configuration

The following steps must be completed to comply with the Evaluated Configuration.

5.5.2.1 As required for **[DB.IA-3]**, database administrators shall set the following initialization parameter:

```
o7_dictionary_accessibility = FALSE
```

5.5.2.2 As required for **[DB.IA-7]**, database administrators shall set the following initialization parameter:

```
sql92_security = TRUE
```

5.5.2.3 As required for **[DB.IA-14]**, database administrators shall set the following initialization parameter:

```
remote_login_passwordfile = 'EXCLUSIVE'
```

5.5.2.4 As required for **[DB.AA-2]**, the `audit_trail` parameter in the appropriate initialization parameter file for that O-RDBMS shall be assigned in one of the following two ways:

```
audit_trail = OS
audit_trail = DB
```

5.5.2.5 As required for **[DB.AA-10]**, if fine-grained auditing is in use then database administrators shall set the `optimizer_mode` initialization parameter in set in one of the following ways:

```
optimizer_mode = first_rows_n (where n =
1,10,100,1000), or
optimizer_mode = all_rows
```

5.5.2.6 As required for **[DB.AA-7],** database administrators shall ensure that session auditing is enabled at all times, by issuing the following statement from an administrative connection to the database:

```
audit session;
```

5.5.2.7 As required for **[DB.AC-7]**, the following SQL statements shall be executed from an administrative connection to the database:

```
revoke execute on dbms_job from public;

revoke execute on utl_smtp from public;

revoke execute on utl_tcp from public;

revoke execute on utl_http from public;

revoke execute on utl_file from public;

revoke execute on dbms_random from public;
```

5.5.2.8 As required for **[DB.IA-1]** the administrator shall ensure OS authentication is not configured for any user connecting to the TOE, i.e. all database users must be configured to have a *database password.* This can be checked at any time by executing:

```
select username from dba_users where password='EXTERNAL';
```

If no records are selected, then all users are authenticating via a database password.

5.5.2.9 As required for **[DB.IA-4]**, all pre-defined accounts (such as SYS, MDSYS, LBACSYS, SYSTEM etc.) and any demonstration accounts (such as SCOTT) created during installation shall have their passwords changed.

If the account is not to be used then it shall be locked and expired. To prevent inappropriate access to the data dictionary tables or other tampering with the database, the passwords set for SYS, LBACSYS and SYSTEM shall be divulged only to the group of administrators who are intended to use them.

5.5.2.10 As required for **[DB.IA-4]**, the following SQL statements shall be executed from an administrative connection to the database:

```
alter user dbsnmp account lock password expire;
```

5.5.2.11 As required for **[DB.IA-18]**, after creating and setting up a database, the default profile must be changed as described in Annex A.

5.5.3 Maintaining the Evaluated Configuration

The above steps are necessary for achieving an initial evaluated configuration. The remaining configuration requirements in this document (Sections 4.1.2, 4.1.3, 4.1.4, 4.1.5, 4.1.6, 4.1.7, 4.1.8 and **[DB.NS-7]**) cover the general administration of the TOE in order that the evaluated configuration is maintained.

5.6 Configuration of Oracle Label Security

No further configuration of Oracle Label Security is required upon installation.

5.7 Client Installation

The TOE scope does not include any Oracle client software, but to set up the test environment for the evaluated configuration, client installation was completed as follows:

- Install the host operating system as described in and section 5.1 above;
- Install the client Oracle software as described in section 5.8 below;
- Configure the network services configuration parameters as described in **[DB.NS-3]** and **[DB.NS-4]**;
- Protect the client applications from unauthorised use by setting the appropriate access control permissions.

Note that untrusted users of the TOE are not expected to be administrators of their local machines.

5.8 Oracle Client Applications

[DB.CA-1] In the test environment for the evaluated configuration the client applications were installed using the Oracle Universal Installer. The following software components shall be selected and installed using the Custom Installation option:

Oracle Database 10*g* Client 10.1.0.3.0
Oracle Network Utilities 10.1.0.3.0
Oracle Database Utilities 10.1.0.3.0
SQL*Plus 10.1.0.3.0
Oracle Call Interface 10.1.0.3.0

Annex B contains a complete list of all the software components that are then installed by the Oracle Universal Installer.

[DB.CA-2] No database applications except those based on OCI (e.g. SQL*Plus) shall be permitted to run on any client or server host machines which access the network, unless they have been shown not to compromise the TOE's security objectives as stated in the [DBPP] and the [ST] (see **[OS.CA-1]**).

This Page Intentionally Blank

ANNEX

A

Password Profile Controls

This Annex specifies the password control requirements that must be applied to all profiles in the evaluated configuration of the TOE. Assertion **[DB.IA-18]** states that the password control limits specified in this Annex must be applied to the default profile as part of the installation task, and then to all new profiles created subsequently.

This Annex does however provide database administrators with a choice of two profiles, both of which provide password controls that are strong enough to meet the claimed CC Strength of Function rating of SOF-*high*. Both choices can also be strengthened further, if necessary, however administrators should see the guidance in section 2.2 of this document, and carefully consider their security requirements and the implications of the profile changes before implementing any such changes.

The two profiles suggested below, entitled ProfileA and ProfileB, require creation via a SQL script (which could be achieved by modifying an example script supplied with the TOE), as well as execution of the script and a SQL statement in the database. The steps are explained fully in Sections A.2 and A.3. A rationale for the two choices available is provided in section A.1.

ProfileA and ProfileB were used during the evaluation of the TOE, along with variants of them that added strengthened password controls. Any installation of the TOE can remain within the TOE's Evaluated Configuration provided that ProfileA or ProfileB are used or, if variants of them are used, then it must be possible to show that the changes have added strengthened password controls.

A.1 Rationale

ProfileA specifies a complexity check function that enforces a minimum password length of 8 characters. It is intended that this profile achieves the required strength by enforcement of password length alone, thereby presenting an attacker with an unreasonably large password space to search. This type of profile may be preferred by ad-

ministrators who do not wish to use any type of lockout on user accounts, i.e. for availability reasons.

Profile B specifies a complexity check function that enforces a minimum password length of 6 characters, plus a 1 minute lockout whenever 3 consecutive failed log in attempts are made. The rationale for this profile is that administrators may not want to mandate a length of 8 for user passwords, but by reducing this to a length of 6 the profile is strengthened by introducing a temporary lockout. This type of lockout works extremely effectively against automated attacks by almost nullifying the speed advantage they would have over manual attacks. The temporary nature of the lockout (one minute is suggested as being sufficient, although a longer time would strengthen this profile) counters a denial of service attack, since the accounts automatically re-enable themselves after the lockout time expires.

The complexity check function for both profiles will do the following checks:

- Check that the password supplied is not the same as the username;
- Check the length of the password meets the minimum requirement;
- Raise application errors if either of these two checks fail.

The two sections for ProfileA and ProfileB below both specify in full the `CREATE FUNCTION` statement that will create a PL/SQL function to be the complexity check. This function can either be created by entering the full creation statement into the database, or by putting it into a SQL script and executing this within the database. The ProfileA and ProfileB sections also specify the SQL statement that can then be used to modify or create profiles to incorporate the new complexity check function.

As a further alternative to creating a script from scratch (by using a text editor), the example complexity check function supplied with the TOE can be modified. The example script supplied is called *utlpwdmg.sql*, and instructions for modifying this (as an alternative to using the scripts in Sections A.2 and A.3) are given in section A.4 below.

A.2 ProfileA

To implement ProfileA, the complexity check function needs to be created, and then assigned to the profile.

Section A.2.1 supplies a listing for a SQL script that, when executed, will create the function. Note, the function can also be entered directly into the database if required (omit the `Rem` statements), however a script is recommended as this will preserve the function definition for future use or modification.

A.2.1 Script Listing

```
Rem Oracle Database 10g Release 1(10.1.0) evaluated configura-
tion
Rem Password complexity check (ProfileA)

CREATE OR REPLACE FUNCTION profilea

(username varchar2,

  password varchar2,

  old_password varchar2)

  RETURN boolean IS
```

```
n boolean;
BEGIN
Rem Check if the password is the same as the username
   IF password = username THEN
     raise_application_error(-20001, 'Password same as user');
   END IF;
Rem Check for the minimum length of the password
   IF length(password) < 8 THEN
     raise_application_error(-20002, 'Password length less than
8');
   END IF;
RETURN(TRUE);
END;
/
```

A.2.2 Database commands

To create the function from a script, the script must be executed in the database by an administrator (e.g. *sys*) as follows:

```
sqlplus> @profilea.sql
```

Once the complexity check function (called `profilea`) is created, then the default profile can be amended as follows:

```
alter profile default limit
password_verify_function profilea;
```

A.3 ProfileB

To implement ProfileB the complexity check function needs to be created and then assigned to the profile in conjunction with other profile limits.

Section A.3.1 supplies a listing for a SQL script that, when executed, will create the function. Note, the function can also be entered directly into the database if required (omit the `Rem` statements), however a script is recommended as this will preserve the function definition for future use or modification.

A.3.1 Script Listing

```
Rem Oracle Database 10g Release 1(10.1.0) evaluated configura-
tion
Rem Password complexity check (ProfileB)
CREATE OR REPLACE FUNCTION profileb
(username varchar2,
  password varchar2,
  old_password varchar2)
  RETURN boolean IS
   n boolean;
```

```
BEGIN
Rem Check if the password is the same as the username
   IF password = username THEN
     raise_application_error(-20001, 'Password same as user');
   END IF;
Rem Check for the minimum length of the password
   IF length(password) < 6 THEN
     raise_application_error(-20002, 'Password length less than
6');
   END IF;
RETURN(TRUE);
END;
/
```

A.3.2 Database Commands

To create the function from a script, the script must be executed in the database by an administrator (e.g. *sys*) as follows:

```
sqlplus> @profileb.sql
```

Once the complexity check function (called `profileb`) is created, then the default profile can be amended as follows:

```
alter profile default limit
failed_login_attempts 3
password_lock_time 1/1440
password_verify_function profileb;
```

A.4 Modifying utlpwdmg.sql

As an alternative to creating the function using the scripts described above, it is also possible to modify the *utlpwdmg.sql* script as described below.

1. In the check for minimum length of password, modify the value of '4' to either '8' (for ProfileA) or '6' (for ProfileB). Ensure this value is changed in two places - the line commencing `IF length`... and the line commencing `raise_application_error`.

2. Comment out all checks except the first two checks (the code for the first two checks ensures that the password is not the same as the username, and that the minimum length of password is met). Note, all lines of code under every check description should be commented out by placing the word "Rem" at the start of the line.

3. Ensure that having commented out every check underneath the first two, that the following lines at the end of the function remain un-commented out:

```
RETURN(TRUE);
END;
/
```

4. Comment out all the lines of the `ALTER PROFILE` statement at the end of the script by placing the word “Rem” at the start of each line.

5. Save the modified script (it is recommended that a different filename is used e.g. `profilea.sql` or `profileb.sql`). Then using a tool such as SQL*PLUS, connect as a privileged user (e.g. *sys*) and run the script to create the complexity check function as follows:

```
sqlplus> @profilea.sql
```

6. The default profile can then be modified to include the complexity check function as follows:

```
sqlplus> alter profile default limit
password_verify_function profilea;
```

This Page Intentionally Blank

ANNEX

B TOE Components

B.1 Database Server Components on Red Hat Linux

The following is a summary of all the software components that are installed on the Red Hat Linux server by the Oracle Universal Installer during the installation of the Oracle Database 10*g* as per Chapter 4 of this document:

- Advanced Queueing (AQ) API 10.1.0.3.0
- Advanced Queueing (AQ) API Patch 10.1.0.4.0
- Advanced Replication 10.1.0.3.0
- Advanced Replication Patch10.1.0.4.0
- Agent Required Support Files 10.1.0.3.0
- Agent Required Support Files Patch 10.1.0.4.0
- Assistant Common Files 10.1.0.3.0
- Assistant Common Files Patch 10.1.0.4.0
- Bali Share 1.1.18.0.0
- CSS Single-Instance Common Files 10.1.0.3.0
- CSS Single-Instance Common Files Patch 10.1.0.4.0
- Character Set Migration Utility 10.1.0.3.0
- Character Set Migration Utility Patch 10.1.0.4.0
- DBJAVA Required Support Files 10.1.0.3.0
- DBJAVA Required Support Files Patch 10.1.0.4.0
- Data Management Services Common Files 10.1.0.3.0
- Data Management Services Common Files 10.1.0.4.0
- Database Configuration Assistant 10.1.0.3.0

- Database Configuration Assistant 10.1.0.4.0
- Database SQL Scripts 10.1.0.3.0
- Database SQL Scripts Patch 10.1.0.4.0
- Database Upgrade Assistant 10.1.0.3.0
- Database Upgrade Assistant Patch 10.1.0.4.0
- Database Verify Utility 10.1.0.3.0
- Database Verify Utility Patch 10.1.0.4.0
- Database Workspace Manager 10.1.0.3.0
- Database Workspace Manager Patch 10.1.0.4.0
- Documentation Required Support Files 10.1.0.3.0
- Enterprise Edition Options 10.1.0.3.0
- Enterprise Manager Agent 10.1.0.3.0
- Enterprise Manager Common Files 10.1.0.3.0
- Enterprise Manager Repository Files 10.1.0.3.0
- Enterprise Manager Minimal Integration 10.1.0.3.0 Beta
- Enterprise Manager plugin Common Files 10.1.0.3.0 Beta
- Enterprise Manager plugin Common Files 10.1.0.4.0
- Export/Import 10.1.0.3.0
- Export/Import 10.1.0.4.0
- Extended Windowing Toolkit 3.3.18.0.0 Beta
- External Naming: NIS 10.1.0.3.0
- External Naming: NIS Patch 10.1.0.4.0
- Generic Connectivity Common Files 10.1.0.3.0
- Generic Connectivity Common Files Patch 10.1.0.4.0
- Generic Connectivity Using ODBC 10.1.0.3.0
- Generic Connectivity Using ODBC Patch 10.1.0.4.0
- Installation Common Files 10.1.0.3.0
- Installation Common Files Patch 10.1.0.4.0
- Installer SDK Component 10.1.0.3.0
- JDBC Common Files 10.1.0.3.0
- JDBC Common Files Patch 10.1.0.4.0
- JDBC/OCI Common Files 10.1.0.3.0
- JDBC/OCI Common Files Patch 10.1.0.4.0
- JDBC/OCI Common Files for Instant Client 10.1.0.3.0
- JDBC/OCI Common Files for Instant Client Patch 10.1.0.4.0

- Java Naming and Directory Interface Libraries 10.1.0.3.0
- Java Naming and Directory Interface Libraries 10.1.0.4.0
- Java Runtime Environment 1.4.2.0.0
- Java Runtime Environment 1.4.2.0.4
- LDAP Required Support Files 10.1.0.3.0
- LDAP Required Support Files Patch 10.1.0.4.0
- Netca Patch 10.1.0.4.0
- New Database ID 10.1.0.3.0
- New Database ID Patch 10.1.0.4.0
- Oracle Call Interface (OCI) 10.1.0.3.0
- Oracle Call Interface (OCI) Patch 10.1.0.4.0
- Oracle Client Required Support Files 10.1.0.3.0
- Oracle Client Required Support Files Patch 10.1.0.4.0
- Oracle Code Editor 1.2.1.0.0I
- Oracle Containers for Java 10.1.0.3.0
- Oracle Containers for Java Patch 10.1.0.4.0
- Oracle Core Required Support Files 10.1.0.3.0
- Oracle Core Required Support Files 10.1.0.4.0
- Oracle Data Mining 10.1.0.3.0
- Oracle Data Mining Patch 10.1.0.4.0
- Oracle Database 10*g* 10.1.0.3.0
- Oracle Database 10*g* 10.1.0.3.0
- Oracle Database 10*g* Patch 10.1.0.4.0
- Oracle Database Patchset 2 10.1.0.4.0
- Oracle Database User Interface 2.2.13.0.0
- Oracle Database Utilities 10.1.0.3.0
- Oracle Database Utilities Patch 10.1.0.4.0
- Oracle Display Fonts 9.0.2.0.0
- Oracle Extended Windowing Toolkit 3.4.28.0.0
- Oracle Globalization Support Patch 10.1.0.3.0
- Oracle Globalization Support Patch 10.1.0.4.0
- Oracle Help For Java 4.2.5.0.0a
- Oracle Help for the Web 1.1.7.0.0a
- Oracle Ice Browser 5.2.3.3.0
- Oracle Internet Directory Client 10.1.0.3.0

- Oracle Internet Directory Client 10.1.0.4.0
- Oracle Internet Directory Client Common Files 10.1.0.3.0
- Oracle Internet Directory Client Common Files Patch 10.1.0.4.0
- Oracle Internet Directory Tools 10.1.0.3.0
- Oracle Internet Directory Tools Patch 10.1.0.4.0
- Oracle JDBC Thin Driver for JDK 1.2 10.1.0.3.0
- Oracle JDBC Thin Driver for JDK 1.2 10.1.0.4.0
- Oracle JDBC Thin Driver for JDK 1.2 Patch 10.1.0.4.0
- Oracle JDBC Thin Driver for JDK 1.4 10.1.0.3.0
- Oracle JDBC Thin Driver for JDK 1.4 10.1.0.4.0
- Oracle JDBC Thin Driver for JDK 1.4 for Instant Client 10.1.0.3.0
- Oracle JDBC Thin Driver for JDK 1.4 for Instant Client 10.1.0.4.0
- Oracle JDBC/OCI Driver for JDK 1.4 10.1.0.3.0
- Oracle JFC Extended Windowing Toolkit 4.2.18.0.0
- Oracle JVM 10.1.0.3.0
- Oracle JVM Patch 10.1.0.4.0
- Oracle Java Tools 10.1.0.3.0
- Oracle Java Tools Patch 10.1.0.4.0
- Oracle Label Security 10.1.0.3.0
- Oracle Label Security 10.1.0.4.0
- Oracle Locale Builder 10.1.0.3.0
- Oracle Locale Builder Patch 10.1.0.4.0
- Oracle Message Gateway Common Files 10.1.0.3.0
- Oracle Net 10.1.0.3.0
- Oracle Net Patch 10.1.0.4.0
- Oracle Net Configuration Assistant 10.1.0.3.0
- Oracle Net Listener 10.1.0.3.0
- Oracle Net Listener Patch 10.1.0.4.0
- Oracle Net Manager 10.1.0.3.0
- Oracle Net Manager Patch 10.1.0.4.0
- Oracle Net Required Support Files 10.1.0.3.0
- Oracle Net Required Support Files Patch 10.1.0.4.0
- Oracle Net Services 10.1.0.3.0
- Oracle Notification Services 9.0.4.0.0
- Oracle One-Off Patch Installer 10.1.0.3.0

- Oracle RAC Required Support Files 10.1.0.3.0
- Oracle RAC Required Support Files Patch 10.1.0.4.0
- Oracle RAC Required Support Files-HAS 10.1.0.3.0
- Oracle RAC Required Support Files-HAS Patch 10.1.0.4.0
- Oracle Starter Database 10.1.0.3.0
- Oracle Starter Database Patch 10.1.0.4.0
- Oracle Text 10.1.0.3.0
- Oracle Text Patch 10.1.0.4.0
- Oracle UIX 2.1.21.0.0a
- Oracle Ultra Search Common Files 10.1.0.3.0
- Oracle Ultra Search Common Files Patch 10.1.0.4.0
- Oracle Ultra Search Middle-Tier 10.1.0.3.0
- Oracle Ultra Search Middle-Tier Patch 10.1.0.4.0
- Oracle Ultra Search Server 10.1.0.3.0
- Oracle Ultra Search Server RDBMS 10.1.0.3.0
- Oracle Ultra Search Server Patch 10.1.0.4.0
- Oracle Universal Installer 10.1.0.3.0
- Oracle Universal Installer 10.1.0.4.0
- Oracle XML SQL Utility 10.1.0.3.0
- Oracle XML SQL Utility Patch 10.1.0.4.0
- Oracle Intermedia 10.1.0.3.0
- Oracle Intermedia Annotator 10.1.0.3.0
- Oracle Intermedia Annotator Patch 10.1.0.4.0
- Oracle Intermedia Audio 10.1.0.3.0
- Oracle Intermedia Audio Patch 10.1.0.4.0
- Oracle Intermedia Client Compatibility Files 10.1.0.3.0
- Oracle Intermedia Client Demos 10.1.0.3.0
- Oracle Intermedia Client Demos Patch 10.1.0.4.0
- Oracle Intermedia Client Option 10.1.0.3.0
- Oracle Intermedia Common Files 10.1.0.3.0
- Oracle Intermedia Common Files Patch 10.1.0.4.0
- Oracle Intermedia Image 10.1.0.3.0
- Oracle Intermedia Image Patch 10.1.0.4.0
- Oracle Intermedia Java Advanced Imaging 10.1.0.3.0
- Oracle Intermedia Java Advanced Imaging Patch 10.1.0.4.0

- Oracle Intermedia Java Client 10.1.0.3.0
- Oracle Intermedia Java Client Patch 10.1.0.4.0
- Oracle Intermedia Locator 10.1.0.3.0
- Oracle Intermedia Locator Patch 10.1.0.4.0
- Oracle Intermedia Video 10.1.0.3.0
- Oracle Intermedia Video Patch 10.1.0.4.0
- Oracle Intermedia Web Client 10.1.0.3.0
- Oracle 10*g* Real Application Clusters Common Files 10.1.0.3.0
- Oracle 10*g* Real Application Clusters Common Files 10.1.0.4.0
- PL/SQL 10.1.0.3.0
- PL/SQL 10.1.0.4.0
- PL/SQL Embedded Gateway 10.1.0.3.0
- PL/SQL Embedded Gateway Patch 10.1.0.4.0
- PL/SQL Required Support Files 10.1.0.3.0
- PL/SQL Required Support Files 10.1.0.4.0
- Parser Generator Required Support Files 10.1.0.3.0
- Parser Generator Required Support Files Patch 10.1.0.4.0
- Patch for Sun JDK 1.4.2.0.4
- Platform Required Support Files 10.1.0.3.0
- Platform Required Support Files Patch 10.1.0.4.0
- Precompiler Required Support Files 10.1.0.3.0
- Precompiler Required Support Files Patch 10.1.0.4.0
- RDBMS Required Support Files 10.1.0.3.0
- RDBMS Required Support Files Patch 10.1.0.4.0
- Recovery Manager 10.1.0.3.0
- Recovery Manager Patch 10.1.0.4.0
- Required Support Files 10.1.0.3.0
- SQL*Loader 10.1.0.3.0
- SQL*Loader 10.1.0.4.0
- SQL*Plus 10.1.0.3.0
- SQL*Plus 10.1.0.4.0
- SQL*Plus Required Support Files 10.1.0.3.0
- SQL*Plus Required Support Files Patch 10.1.0.4.0
- SQLJ Runtime 10.1.0.3.0
- SQLJ Runtime Patch 10.1.0.4.0

- Secure Socket layer 10.1.0.3.0
- Secure Socket layer Patch 10.1.0.4.0
- SSL Required Support Files 10.1.0.3.0
- SSL Required Support Files Patch 10.1.0.4.0
- SSL Required Support for InstantClient 10.1.0.3.0
- SSL Required Support for InstantClient Patch 10.1.0.4.0
- Sample Schema 10.1.0.3.0
- Sample Schema Patch 10.1.0.4.0
- Sun JDK 1.4.2.0.1
- Sun JDK Patch 1.4.2.0.4
- Sun JDK Extensions 9.0.4.0.0
- Utilities Common Files 10.1.0.3.0
- Utilities Common Files Patch 10.1.0.4.0
- Visigenics ORB 3.4.0.0.0
- Visigenics ORB 3.4.0.0.0c
- XDK Required Support Files 10.1.0.3.0
- XDK Required Support Files Patch 10.1.0.4.0
- XML 10.1.0.3.0
- XML Patch 10.1.0.4.0
- XML Class Generator for Java 10.1.0.3.0
- XML Class Generator for Java Patch 10.1.0.4.0
- XML Parser for Java 10.1.0.3.0
- XML Parser for Java Patch 10.1.0.4.0
- XML Parser for Oracle JVM 10.1.0.3.0
- XML Parser for Oracle JVM Patch 10.1.0.4.0
- XML Parser for PL/SQL 10.1.0.3.0
- XML Patch 10.1.0.4.0
- XML Transviewer Beans 10.1.0.3.0
- XML Transviewer Beans Patch 10.1.0.4.0
- XML Transx 10.1.0.3.0
- XML Transx Patch 10.1.0.4.0
- XSQL Servlet 10.1.0.3.0
- XSQL Servlet Patch 10.1.0.4.0
- regexp 2.1.9.0.0

B.2 Evaluated Configuration Boundaries

SQL*Plus is used by the evaluators for testing the TOE components. However, it is not part of the evaluated configuration.

[DB-4] The evaluated configuration of the TOE on the Red Hat Linux System shall comprise exactly the following software components:

- Assistant Common Files 10.1.0.3.0
- Assistant Common Files Patch 10.1.0.4.0
- Generic Connectivity Common Files 10.1.0.3.0
- Generic Connectivity Common Files Patch 10.1.0.4.0
- Generic Connectivity Using ODBC 10.1.0.3.0
- Generic Connectivity Using ODBC Patch 10.1.0.4.0
- Oracle Net 10.1.0.3.0
- Oracle Net Patch 10.1.0.4.0
- Oracle Net Listener 10.1.0.3.0
- Oracle Net Listener Patch 10.1.0.4.0
- Oracle Net Manager 10.1.0.3.0
- Oracle Net Manager Patch 10.1.0.4.0
- Oracle Net Required Support Files 10.1.0.3.0
- Oracle Net Required Support Files Patch 10.1.0.4.0
- Oracle Net Services 10.1.0.3.0
- Oracle Core Required Support Files 10.1.0.3.0
- Oracle Core Required Support Files 10.1.0.4.0
- Oracle Call Interface 10.1.0.3.0
- Oracle Call Interface Patch 10.1.0.4.0
- Oracle Database 10*g* 10.1.0.3.0
- Oracle Database 10*g* Patch 10.1.0.4.0
- Oracle Label Security 10.1.0.3.0
- Oracle Label Security 10.1.0.4.0
- Parser Generator Required Support Files 10.1.0.3.0
- Parser Generator Required Support Files Patch 10.1.0.4.0
- PL/SQL 10.1.0.3.0
- PL/SQL 10.1.0.4.0
- PL/SQL Embedded Gateway 10.1.0.3.0
- PL/SQL Embedded Gateway Patch 10.1.0.4.0
- PL/SQL Required Support Files 10.1.0.3.0

- PL/SQL Required Support Files 10.1.0.4.0
- Platform Required Support Files 10.1.0.3.0
- Platform Required Support Files Patch 10.1.0.4.0
- RDBMS Required Support Files 10.1.0.3.0
- RDBMS Required Support Files Patch 10.1.0.4.0
- Required Support Files 10.1.0.3.0

The TOE consists of the Database Server software which receives database access requests via the Oracle Call Interface. This software performs the required read and write operations on database objects and returns data and results to the user, in accordance with the user's database object access privileges and other constraints configured by a database administrative user. The components listed above include the items required for the setting up and running of tests of the TOE during its evaluation.

B.3 Client components

There are no client components in the TOE.

The following is a list of all the software components that were installed on the client running SuSE Linux 9 by the Oracle Universal Installer during the installation of the client software as per **[DB.CA-1]** for use in testing the TOE in its evaluated configuration.

- Advanced Queueing (AQ) API 10.1.0.3.0
- Agent Required Support Files 10.1.0.3.0
- Assistant Common Files 10.1.0.3.0
- Bali Share 1.1.18.0.0
- Character Set Migration Utility 10.1.0.3.0
- CSS Single-Instance Common Files 10.1.0.3.0
- DBJAVA Required Support Files 10.1.0.3.0
- Documentation Required Support Files 10.1.0.3.0
- Enterprise Manager Minimal Integration 10.1.0.3.0 Beta
- Enterprise Manager plugin Common Files 10.1.0.3.0 Beta
- Export/Import 10.1.0.3.0
- Installation Common Files 10.1.0.3.0
- Installer SDK Component 10.1.0.3.0
- Java Runtime Environment 1.4.2.0.0
- LDAP Required Support Files 10.1.0.3.0
- Object Type Translator 10.1.0.3.0
- Oracle Call Interface (OCI) 10.1.0.3.0
- Oracle C++ Call Interface 10.1.0.3.0

- Oracle C++ Call Interface for InstantClient 10.1.0.3.0
- Oracle Client Required Support Files 10.1.0.3.0
- Oracle Code Editor 1.2.1.0.0I
- Oracle Core Required Support Files 10.1.0.3.0
- Oracle Database Utilities 10.1.0.3.0
- Oracle Display Fonts 9.0.2.0.0
- Oracle Extended Windowing Toolkit 3.4.28.0.0
- Oracle Globalisation Support 10.1.0.3.0
- Oracle Help For Java 4.2.5.0.0a
- Oracle Ice Browser 5.2.3.3.0
- Oracle Locale Builder 10.1.0.3.0
- Oracle JFC Extended Windowing Toolkit 4.2.18.0.0
- Oracle Net 10.1.0.3.0
- Oracle Net Configuration Assistant 10.1.0.3.0
- Oracle Net Manager 10.1.0.3.0
- Oracle Net Required Support Files 10.1.0.3.0
- Oracle Network Utilities 9.2.0.1.0
- Oracle One-Off Patch Installer 10.1.0.3.0
- Oracle RAC Required Support Files 10.1.0.3.0
- Oracle RAC Required Support Files-HAS 10.1.0.3.0
- Oracle Real Application Clusters Common Files 10.1.0.3.0
- Oracle Required Support Files 32 Bit 10.1.0.3.0
- Oracle UIX 2.21.0.0a
- Oracle Client 10.1.0.3.0
- PL/SQL Required Support Files 10.1.0.3.0
- Parser Generator Required Support Files 10.1.0.3.0
- Platform Required Support Files 10.1.0.3.0
- Precompiler Common Files 10.1.0.3.0
- Precompiler Required Support Files 10.1.0.3.0
- RDBMS Required Support Files 10.1.0.3.0
- Recovery Manager 10.1.0.3.0
- Required Support Files 10.1.0.3.0
- SQL*Plus 10.1.0.3.0
- SQL*Plus Required Support Files 10.1.0.3.0
- SSL Required Support Files 10.1.0.3.0

- SSL Required Support Files for InstantClient 10.1.0.3.0
- Sun JDK 1.4.2.0.1
- Sun JDK Extensions 9.0.4.0.0
- Utilities Common Files 10.1.0.3.0
- XDK Required Support Files 10.1.0.3.0
- regexp 2.1.9.0.0

This Page Intentionally Blank

ANNEX

C Red Hat Linux Packages

C.1 Installed Packages

Oracle Database 10*g* Release 1 (10.1.0.4) was installed on Red Hat Linux in accordance with [ORHEL] and configured in accordance with Chapter 4 of this document. All Linux packages were removed from the server except those found within the Evaluated Configuration of Red Hat Linux, as defined in [ECGR], and those needed by Oracle Database 10*g*. The full list of installed Linux packages is provided below:

```
acl-2.2.3-1
apmd-3.0.2-18
ash-0.3.8-16
aspell-0.33.7.1-25
at-spi-1.1.9-1
attr-2.2.0-1
authconfig-4.3.7-1
autoconf-2.57-3
autofs-3.1.7-41
automake-1.6.3-5
basesystem-8.0-2
bash-2.05b-29
bc-1.06-15
beecrypt-3.0.1-0.20030630
bind-utils-9.2.2-21
binutils-2.14.90.0.4-26
```

```
bison-1.875-4
bzip2-1.0.2-11
bzip2-libs-1.0.2-11
chkconfig-1.3.8-3
compat-gcc-7.3-2.96.122
compat-gcc-c++-7.3-2.96.122
compat-libstdc++-7.3-2.96.122
compat-libstdc++-devel-7.3-2.96.122
comps-3as-0.20031007
coreutils-4.5.3-26
cpio-2.5-3
cpp-3.2.3-20
cracklib-2.7-22
cracklib-dicts-2.7-22
crontabs-1.10-5
cups-1.1.17-13.3.6
cups-libs-1.1.17-13.3.6
curl-7.10.6-4.1
cvs-1.11.2-10
cyrus-sasl-2.1.15-3
cyrus-sasl-gssapi-2.1.15-3
cyrus-sasl-md5-2.1.15-3
cyrus-sasl-plain-2.1.15-3
db4-4.1.25-8
dev-3.3.8-1
devlabel-0.41.01-1
dhclient-3.0pl2-6.14
dialog-0.9b-20020814.6
diffutils-2.8.1-8
distcache-0.4.2-3
dosfstools-2.8-10
dump-0.4b28-7
e2fsprogs-1.32-15
ed-0.2-33
eject-2.0.13-2
elfutils-0.89-1
elfutils-libelf-0.89-1
elinks-0.4.2-7
ethtool-1.8-2
expat-1.95.5-6
```

```
expect-5.38.0-92
fbset-2.1-13
file-3.39-9
filesystem-2.2.1-3
findutils-4.1.7-9
finger-0.17-18
flex-2.5.4a-29
fontconfig-2.2.1-6.0
freetype-2.1.4-4.0
ftp-0.17-17
gawk-3.1.1-9
gcc-3.2.3-20
gcc-c++-3.2.3-20
gcc-c++-ssa-3.5ssa-0.20030801.41
gdbm-1.8.0-20
gettext-0.11.4-7
glib-1.2.10-11.1
glib2-2.2.3-2.0
glibc-2.3.2-95.3
glibc-common-2.3.2-95.3
glibc-devel-2.3.2-95.3
glibc-headers-2.3.2-95.3
glibc-kernheaders-2.4-8.34
gmp-4.1.2-5
gnupg-1.2.1-4
gpm-1.19.3-27.2
grep-2.5.1-16
groff-1.18.1-27
grub-0.93-4
gzip-1.3.3-9
hdparm-5.4-1
hesiod-3.0.2-28
hotplug-2002_04_01-20
htmlview-2.0.0-10
hwdata-0.98-1
info-4.5-3
initscripts-7.31.6.EL-1
iproute-2.4.7-10
ipsec-tools-0.2.2-7
iptables-1.2.8-12
```

```
iptables-ipv6-1.2.8-12
iputils-20020927-11
irda-utils-0.9.15-1
isdn4k-utils-3.1-76
jfsutils-1.1.2-2
jwhois-3.2.2-1
kbd-1.08-10.1
kernel-2.4.21-4.EL
kernel-pcmcia-cs-3.1.31-13
kernel-smp-2.4.21-4.EL
kernel-utils-2.4-8.37
krb5-libs-1.2.7-19
krb5-workstation-1.2.7-19
krbafs-1.1.1-11
krbafs-devel-1.1.1-11
krbafs-utils-1.1.1-11
kudzu-1.1.21-1
less-378-11
lftp-2.6.3-3
lha-1.14i-10
libacl-2.2.3-1
libaio-0.3.96-3
libattr-2.2.0-1
libcap-1.10-15
libgcc-3.2.3-20
libgcj-3.2.3-20
libgcj-ssa-devel-3.5ssa-0.20030801.41
libjpeg-6b-30
libpng-1.2.2-16
libstdc++-3.2.3-20
libstdc++-devel-3.2.3-20
libstdc++-ssa-3.5ssa-0.20030801.41
libstdc++-ssa-devel-3.5ssa-0.20030801.41
libtermcap-2.0.8-35
libtiff-3.5.7-13
libtool-libs-1.4.3-6
libuser-0.51.7-1
libwvstreams-3.70-10
libxml2-2.5.10-5
lockdev-1.0.1-1.2
```

```
logrotate-3.6.9-1
logwatch-4.3.2-2
losetup-2.11y-31.1
lslk-1.29-8
lsof-4.63-4
lvm-1.0.3-15
m4-1.4.1-13
mailcap-2.1.14-1
mailx-8.1.1-31
make-3.79.1-17
MAKEDEV-3.3.8-1
man-1.5k-10
man-pages-1.60-4.1
mdadm-1.0.1-1
mgetty-1.1.30-3
mingetty-1.06-1
minicom-2.00.0-17.1
mkbootdisk-1.5.1-1
mkinitrd-3.5.13-1
mktemp-1.5-18
modutils-2.4.25-9.EL
mount-2.11y-31.1
mtools-3.9.8-8
mtr-0.52-2
mt-st-0.7-11
nano-1.2.1-4
nc-1.10-18
ncompress-4.2.4-33
ncurses-5.3-9.3
netconfig-0.8.19-1
netdump-0.6.10-2
netpbm-9.24-11
net-tools-1.60-20
newt-0.51.5-1
nfs-utils-1.0.5-3
nscd-2.3.2-95.3
nss_ldap-207-2
ntsysv-1.3.8-3
openldap-2.0.27-11
openldap-clients-2.0.27-11
```

```
openmotif-2.2.2-16
openssh-3.6.1p2-18
openssh-server-3.6.1p2-18
openssl-0.9.7a-22.1
openssl-devel-0.9.7a-22.1
pam_krb5-1.70-1
pam_smb-1.1.7-1
pam-0.75-51
pam-devel-0.75-51
parted-1.6.3-29
passwd-0.68-3
patch-2.5.4-16
pax-3.0-6
pciutils-2.1.10-7
pcre-3.9-10
pdksh-5.2.14-21
perl-5.8.0-88.4
perl-DateManip-5.40-30
perl-Filter-1.29-3
perl-HTML-Parser-3.26-17
perl-HTML-Tagset-3.03-28
perl-libwww-perl-5.65-6
perl-URI-1.21-7
pinfo-0.6.6-4
popt-1.8.1-4.2
portmap-4.0-56
ppp-2.4.1-14
prelink-0.3.0-6
procmail-3.22-9
procps-2.0.13-9.2E
psacct-6.3.2-27
psmisc-21.3-1.RHEL.0
pspell-0.12.2-16.1
pyOpenSSL-0.5.1-8
python-2.2.3-5
python-optik-1.4.1-2
pyxf86config-0.3.5-1
quota-3.09-1
raidtools-1.00.3-7
rdate-1.3-2
```

```
rdist-6.1.5-30
readline-4.3-5
redhat-config-mouse-1.0.13-1
redhat-config-network-tui-1.2.58-1
redhat-config-securitylevel-tui-1.2.9-1
redhat-logos-1.1.14.3-1
redhat-lsb-1.3-3
redhat-menus-0.39-1
redhat-release-3AS-1
rhnlib-1.3-12
rhpl-0.110-1
rmt-0.4b28-7
rootfiles-7.2-6
rpm-4.2.1-4.2
rpm-build-4.2.1-4.2
rpmdb-redhat-3-0.20031007
rpm-python-4.2.1-4.2
rp-pppoe-3.5-4
rsh-0.17-17
rsync-2.5.6-20
schedutils-1.3.0-3
sed-4.0.7-3
setarch-1.3-1
setserial-2.17-12
setup-2.5.27-1
setuptool-1.13-1
shadow-utils-4.0.3-7
sharutils-4.2.1-16
slang-1.4.5-18
slocate-2.6-9
specspo-3EL-1
star-1.5a08-4
strace-4.5-3
stunnel-4.04-4
sudo-1.6.7p5-1
symlinks-1.2-18
sysklogd-1.4.1-12
syslinux-2.06-0.3E
sysreport-1.3.7-1
SysVinit-2.85-4
```

```
talk-0.17-20
tar-1.13.25-13
tcl-8.3.5-92
tcp_wrappers-7.6-34
tcpdump-3.7.2-7
tcsh-6.12-4
telnet-0.17-26
termcap-11.0.1-17.1
texinfo-4.5-3
tftp-0.32-4
time-1.7-23
tmpwatch-2.8.4-5
traceroute-1.4a12-20
tzdata-2003c-1
unzip-5.50-34
up2date-4.0.1-1
urw-fonts-2.1-5.0
usbutils-0.11-1
usermode-1.68-5
utempter-0.5.2-16
util-linux-2.11y-31.1
vconfig-1.6-2
vim-common-6.2.98-1
vim-minimal-6.2.98-1
vixie-cron-3.0.1-74
wget-1.8.2-15
which-2.14-7
wireless-tools-26-2
words-2-21
wvdial-1.53-11
XFree86-libs-4.3.0-35.EL
XFree86-libs-data-4.3.0-35.EL
XFree86-Mesa-libGL-4.3.0-35.EL
xinetd-2.3.12-2.3E
ypbind-1.12-1
yp-tools-2.8-1
zip-2.3-16
zlib-1.1.4-8.1
zlib-devel-1.1.4-8.1
```

C.2 Packages outside Red Hat Evaluated Configuration

The packages not included in [ECGR], but which are mandated by [INST_LINUX_10*g*], are listed in the table below with a brief description.

Package name	Description
compat-gcc	GNU C Compiler required by Oracle.
compat-gcc-c++	C++ Compiler required by Oracle.
glibc-locale	Local data for internationalization features of the GNU C Library. Required by Oracle Database 10*g*.
libaio	Linux native asynchronous I/O access library. Required by Oracle Database 10*g*.
openmotif	Open Motif runtime environment. Required by Oracle Database 10*g*.

Table 5-1: Additional Packages needed by Oracle Database 10g

Note that the GNU C Compiler and C++ Compiler must be installed so that only administrators can execute them.

None of these packages affects the security functionality of the TOE when running in its evaluated configuration.

This Page Intentionally Blank

ANNEX

D References

[ADG] *Oracle Database Application Developer's Guide - Fundamentals,* 10*g*, Release 1 (10.1), Oracle Corporation.

[CC] *Common Criteria for Information Technology Security Evaluation*, Version 2.2, ISO/IEC 15408, CCIMB-2004-01-001, January 2004

[CPU Notes] Oracle Critical Patch Update July 2005
Release Notes for Oracle Database Server Version (10.1.0.4), README for 4392423
Available from Oracle Metalink (http://metalink.oracle.com). Click Patches and Updates from side-panel then search by Patch Number 4392423. Click on "View Readme").

[DAG] *Oracle Database Administrator's Guide*, 10*g Release 1 (10.1)*, Oracle Corporation.

[DBPP] *Database Management System Protection Profile,* Version 2.1, May 2000

[OLSECD_10] *OLS Evaluated Configuration for Oracle9i*, *Release 2 (9.2.0)*, Issue 1.0, Oracle Corporation

[ECGR] *EAL3 Evaluated Configuration Guide for Red Hat Enterprise Linux*, Klaus Weidner, June 29, 2004, version 1.2.
Available from ftp://www6.software.ibm.com/software/developer/library/os-ltc-security/RHEL-EAL3-Configuration-Guide.pdf

[INST_LINUX_10*g*] *Oracle Database Installation Guide 10g Release 1 (10.1.0.3) for Linux x86-64*, Oracle Corporation

[ORHEL] *Deploying Oracle9i Database on Red Hat Enterprise Linux,* By Jennifer Lamb, Red Hat Inc., March 2004
Available from http://www.RedHat.com

[PSN-Linux] Oracle Database Patch Set Notes, 10*g* Release 1 (10.1.0.4), Patch Set 2 for Linux x86, Oracle Corporation. Available from http://metalink.oracle.com via the Patches and Updates section.

[ST] *OLS Security Target for Oracle Database 10g, Release 1 (10.1.0),* Oracle Corporation

[SG] *Oracle Database Security Guide, 10g Release 1 (10.1)*, Oracle Corporation.