



Statement of Direction

Security Evaluations

July 2007

Introduction

Security evaluation is a process by which independent bodies provide confidence in the security of Information Technology products and systems to commercial, government and military institutions. In conjunction with the criteria upon which it is based, independent security evaluation provides a framework of assurance for purchasers and vendors alike.

Oracle Corporation, as the leading supplier of secure database technology, is committed to providing its customers with independently evaluated secure products. To this end, Oracle is currently undergoing several official international security evaluations of its products and has successfully completed over 25 evaluations to date.

Future plans include continuing to evaluate Oracle Database including the addition of database options such as Real Application Clusters and Database Vault, Oracle middleware products centered on Oracle Application Server, security relevant Oracle applications products, and Oracle's Linux distribution, Oracle Enterprise Linux. The platforms on which evaluations take place now include evaluated versions of Linux as well as Sun Solaris. No further evaluations will take place on Microsoft Windows platforms.

Oracle's ongoing commitment to current and evolving international security standards places Oracle at the forefront of open secure technology.

Evaluation Criteria

International Common Criteria

The *International Common Criteria for Information Technology Security Evaluation (CC)* is a joint effort between nations to develop a single framework of mutually recognized evaluation criteria. The CC provides a collection of Evaluation Assurance Levels (EAL) ranging from EAL1 (lowest) through EAL7 (highest) to be awarded to products and systems upon successful completion of evaluation. The CC is an ISO standard (number 15408). There are currently 24 nations that mutually recognize CC evaluations up to EAL4 under the CC Recognition Arrangement.

US FIPS 140-2

The *Federal Information Processing Standard (FIPS) PUB 140-2 (which supercedes 140-1), Security Requirements for Cryptographic Modules*, was established to validate encryption products purchased by the U.S. and Canadian governments. Products are validated against FIPS 140-2 at security levels, ranging from level 1 (lowest) through level 4 (highest).

Note that FIPS 140-2 only applies to the cryptographic modules of products.

Oracle has completed one FIPS 140-1 validation and two FIPS 140-2 validations and will continue to validate to FIPS 140-2 for cryptographic modules used by the database and middleware products.

Oracle has embraced the CC (and FIPS 140-2 for cryptographic modules) as the primary evaluation criteria for its products. Other evaluation criteria (see below) are now considered obsolete and only Common Criteria and FIPS 140-2 evaluations will be performed in the future.

European ITSEC

The European *Information Technology Security Evaluation Criteria* (ITSEC) resulted from the harmonization of security evaluation criteria of four European nations. The ITSEC defined seven assurance levels from E0 (lowest) through E6 (highest), representing degrees of confidence in the correctness of the product or system. The ITSEC also contained several classes of pre-defined functionality, which map to the U.S. TCSEC Classes. The assurance levels were used in conjunction with the functionality classes to give a product or system a specific security evaluation rating.

Oracle was an active participant in the ITSEC, but will not pursue further ITSEC evaluations as it has been superseded by the Common Criteria.

U.S. TCSEC

The U.S. *Trusted Computer System Evaluation Criteria* (TCSEC), also called the *Orange Book*, was first used in the evaluation of operating systems in the U.S. The *Trusted Database Interpretation* (TDI), also called the *Lavender Book*, was developed to provide an interpretation of these evaluation criteria for database management systems and other layered products. Products were evaluated against the TCSEC/TDI at Classes, which are: D (lowest), C1, C2, B1, B2, B3, and A1 (highest).

Note that the TCSEC standard and related criteria such as the TDI are obsolete. Similarly, the classes D – A1 are obsolete, even though the C2 and B1 requirements are still cited.

Oracle participated in the TCSEC for the very first evaluations of its database server products, but will not pursue further TCSEC evaluations as it is superseded by Common Criteria.

Russian Federation Criteria

The Russian Federation certification criteria consists of a collection of five guiding documents containing certification rules, levels and standards published and overseen by the government institution, Russian Gostekhkommisia (State Technical Commission). Products are certified at security levels ranging from IV (lowest) to I (highest).

Oracle is the first and only database vendor to successfully complete certification of its server products against this criteria. No further Russian Criteria certifications will be undertaken.

<http://www.oracle.com/>

This document is provided for informational purposes only and the information herein is subject to change without notice. Please report any errors herein to Oracle Corporation. Oracle Corporation does not provide any warranties covering and specifically disclaims any liability in connection with this document.

Oracle is a registered trademark of Oracle Corporation.

All other company and product names mentioned are used for identification purposes only, and may be trademarks of their respective owners.

Copyright © Oracle Corporation 2007. All rights reserved.