National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

International Business Machines Corporation, Rochester, MN 55901

Informix Dynamic Server Version 11.5

Report Number: CCEVS-VR-VID10192-2009
Dated: 17 February 2009
Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6757
Fort George G. Meade, MD 20755-6757

ACKNOWLEDGEMENTS

Validation Team

Jandria Alexander
Aerospace Corporation
Columbia, MD

Jean Hung
MITRE Corporation
Bedford, MA

Common Criteria Testing Laboratory

Tammy Compton
Eve Pierre
Katie Sykes
Science Applications International Corporation
Columbia, Maryland

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of IBM Informix Dynamic Server Version 11.5 (Enterprise Editions) (henceforth referred to as IDS). It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Science Applications International Corporation (SAIC) Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, United States of America, and was completed in January 2009. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by SAIC. The evaluation determined that the product is both **Common Criteria Part 2 Extended and Part 3 Conformant**, and meets the assurance requirements of EAL 4 augmented with ALC_FLR.2.

The IBM IDS product is a relational database management system (RDBMS) sold as an application to be installed on a commercial operating system. It is designed primarily to implement databases that can be manipulated using Structured Query Language (SQL) statements.

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 1.0) for conformance to the Common Criteria for IT Security Evaluation (Version 2.3). This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

The validation team monitored the activities of the evaluation team, observed evaluation testing activities, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The SAIC evaluation team concluded that the Common Criteria requirements for Evaluation Assurance Level (EAL 4 augmented with ALC_FLR.2) have been met.

The technical information included in this report was obtained from the IBM Informix Dynamic Server Version 11.5, Security Target and analysis performed by the Validation Team.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE:	IBM Informix Dynamic Server Version 11.5 (Enterprise Editions)
Protection Profile	None
ST:	IBM Informix Dynamic Server Version 11.5 Security Target, Version 1.0, September 25, 2008
Evaluation Technical Report	Evaluation Technical Report for the Informix Dynamic Server Version 11.5 Part 1 (Non-Proprietary), Version 1.0, December 19, 2008; Part 2 (Proprietary), Version 3.0, January 5, 2009.
CC Version	Common Criteria for Information Technology Security Evaluation, Version 2.3 Part 2: Evaluation Methodology, Supplement: ALC_FLR- Flaw Remediation, Version 1.1, February 2002, CEM-2001/0015R
Conformance Result	CC Part 2 conformant, CC Part 3 conformant
Sponsor	IBM
Developer	IBM

Item	Identifier
Common Criteria Testing Lab (CCTL)	SAIC, Columbia, MD
CCEVS Validators	Jandria Alexander, Aerospace Corporation, Columbia, MD
	Jean Hung, MITRE Corporation, Bedford, MA

3 Architectural Information

Note: The following architectural description is based on the description presented in the Security Target.

3.1 TOE Overview

The IDS is an RDBMS designed primarily to implement databases that can be manipulated using Structured Query Language (SQL) statements.

The IDS is an application realized by a collection of cooperating processes. As an application, IDS depends on the underlying operating system for its execution environment and communication services as well as for storage mechanisms for itself, its configuration, and its databases. It also depends on the underlying operating system for protection of its resources for its own protection and also for the differentiation and protection of its clients.

The IDS acts as a server servicing requests of local clients on the same host operating system and on other hosts using network communication mechanisms. The IDS offers a proprietary SQLI protocol to its own clients as well as Distributed Relational Database Architecture (DRDA) support for other clients.

3.2 TOE Architecture

The IDS is a multi-process and multi-threaded application. Each process of the IDS application is referred to as a Virtual Processor (VP) and each VP is designed to fulfill a specific role in implementing the RDBMS. There are VPs specifically designed to handle SQL statements, network communication, local communication, I/O processing, and other miscellaneous functions of IDS. Each of the processes of IDS share memory resources and file descriptors, working as a collective. The processing for a given session can move from VP to VP as necessary. This happens when threads in one VP call threads in another VP to continue a logical thread of execution for the session, utilizing resources (e.g., stack) stored in shared memory. Multiple threads can be used to achieved parallelism for a given session when appropriate (e.g., for parallel sorts and scans). Most of the actual SQL processing is accomplished on CPU VPs using non-preemptive scheduling for threads. When a thread goes into a wait state, the VP switches stacks and continues with another thread.

3.3 Physical Boundaries

The TOE is IBM Informix Dynamic Server Version 11.5. The main program for the IDS, used for all VPs, is ‘oninit’. The TOE includes a number of additional utility programs for

the purposes of managing IDS. A complete list can be found in the administrator guidance documents, but the more security relevant utilities are:

- onmode: provides means to modify behavior and state of the engine; supports adding and dropping of VPs
- onspaces: dbspace (tablespace) and chunk (container) administration
- onparams: provides a means to dynamically add or drop logs
- onaudit: manages audit masks and auditing configuration
- onshowaudit: extracts information from an audit trail
- dbload: load data into a database table
- dbaccess: a client application distributed with the product that facilitates communication between database users (e.g., administrators) and the database VPs

Note that there are other products, including Informix Connect, Informix DataBlade Developer's Kit, Informix Server Administrator (ISA) and Informix Spatial Datablade, associated with IDS (e.g., that may be referenced in guidance documents) that are not included within the TOE because they are separate products subject to separate license requirements.

The IDS is design to operate on a number of UNIX operating systems as well as Microsoft Windows as indicated below:

Version	Platform	Processor Model	OS Build
Sun 32-bit	Solaris	Sparc	Solaris 9, Solaris10
Sun 64-bit	Solaris	Sparc	Solaris 9, Solaris10
Sun 64-bit	Solaris	AMD64 (Opteron)	Solaris 10
HP 32-bit	HP-UX	PA-RISC	HP-UX 11i, HP-UX 11.23PI, 11.31
HP 64-bit	HP-UX	PA-RISC	HP-UX 11i, HP-UX 11.23PI,11.31
HP 64-bit	HP-UX	Itanium	HP-UX 11.23PI, HP-UX 11.31
HP 32-bit	HP-UX	Itanium	HP-UX 11.23PI, HP-UX11.31
IBM 32-bit	AIX	PowerPC	AIX 5L 5.3
IBM 64-bit	AIX	PowerPC	AIX 5L 5.3
Windows	Windows	x86	Windows 2003, Windows XP,Vista
Intel 32-bit	Linux	x86	RHEL 4, SUSE SLES 10, Asianux 2.05
Intel/AMD 32-bit	Linux	x86_64 (EM64T/AMD64)	RHEL 4, SUSE SLES 10, Asianux 2.05
Intel/AMD 64-bit	Linux	x86_64 (EM64T/AMD64)	RHEL 4, SUSE SLES 10, Asianux 2.05
IBM 64-bit	Linux	PowerPC (pSeries/iSeries, OpenPower, JS20	RHEL 4, SUSE SLES 10, Asianux 2.05

Version	Platform	Processor Model	OS Build
		Blades)	
IBM 64-bit	Linux	zSeries	RHEL 4, SUSE SLES 10
Intel 64-bit	Linux	Itanium	RHEL 4, SUSE SLES 10
Solaris Opteron 32 bit client only	Solaris	Opteron	

Table 1 Supported Platforms

Additionally, IDS can be configured to use a pluggable authentication module (PAM) implemented within the IT environment in order to ensure that users are authenticated properly. This is an alternative to relying on authentication that otherwise would be provided by the underlying operating system.

4 Security Policy

The Security Functional Policies (SFPs) implemented by IDS are based upon the basic set of security policies to support data separation: audit, access control, identification and authentication, security management, and protection of the TSF.

Note: Much of the description of the IDS security policy has been extracted and reworked from the IDS Security Target.

4.1 Security Audit

The IDS has the ability to audit security relevant events related to its security functions. An authorized administrator, using the onaudit utility program, can enable and disable the audit feature and can select specifically which security relevant events should be audited based on event type and user.

Audit records are stored within files in the IT environment. The onshowaudit utility allows an authorized administrator to extract the audit records from the audit trail into a file that could potentially be viewed directly using tools available in the IT environment or alternately it can be loaded into an IDS database table, using dbload, so that the features of IDS can be used to more effectively review the audit records with searching and sorting capabilities.

4.2 Access Control

The IDS associates privileges with each individual user. These privileges are associated with operations that can be performed on the objects (e.g., database) that are implemented by the IDS. The IDS uses identities, privileges, and access control lists associated with users and objects to determine whether specific operations will be allowed when attempted by client users.

IDS implements a few roles, each having special privileges that are not available to normal users. These roles are associated with groups defined in the underlying operating system and users are assigned roles by virtue of their membership in those groups. Note that users in these roles can execute certain privileged SQL commands while 'privileges' are associated with access permissions for IDS objects. For this ST, references to the "authorized administrator" role are implemented in the IDS as any of the following roles: Operating System Administrator (OSA), Database System Security Officer (DBSSO), Database System Administrator (DBSA), Database Security Administrator (DBSECADM), or Audit Analysis Officer (AAO). While the IDS offers these different roles with distinct responsibilities, this ST does not make specific role separation claims and hence treats them all logically as a single role – the authorized administrator. References to the "user" role are implemented in the IDS as any user not a member of one of the administrative roles.

In addition to using privileges and authorities to control access, IDS implements a label-based access control (LBAC) mechanism. The IDS DBSECADM can grant (or revoke) security labels and exemptions to (or from) users as well as create and drop LBAC security objects in order to define LBAC polices for specific database tables. Once a table is configured with a LBAC policy (i.e., the table is LBAC protected relative to either rows or columns), users must additionally satisfy the LBAC access rules in order to access or modify the applicable table rows or columns.

4.3 Identification and Authentication

The IDS requires all users to be identified before allowing them access to IDS resources. The IT environment is responsible for user authentication while the IDS requires the user identity returned by the IT environment to associate IDS credentials (e.g., privileges) with the authenticated user.

4.4 Security Management

The IDS includes the roles of authorized administrator and user implemented using IT environment groups, and associated IDS roles (see above) and (access control) privileges, and allows individual users to be assigned to those roles by virtue of the assignment of the applicable groups (in the IT environment) and privileges to their identity. Management of the IDS TOE, including the ability to select and review audit records, is restricted to authorized administrators and access to the TOE (e.g., the utility programs and associated data and configuration files) through its IT environment. Management of the IDS objects is restricted to those users that are assigned the appropriate privileges to do so.

Note that for the most part management of the TOE is accomplished via SQL statements that can be issued interactively using the dbaccess utility.

4.5 Protection of the TOE Security Functions

The IDS executes within processes provided by the host operating system. However, it is designed to not share its process space with non-TOE entities in order to ensure that its

resources are protected. The IDS has been designed so that each of its interfaces performs the necessary access checks before allowing access to IDS resources.

5 Assumptions

The following assumptions were made during the evaluation of IDS:

- There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
- The system administrative personnel are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the administrator documentation.
- Authorized users possess the necessary authorization to access at least some of the information managed by the TOE and are expected to act in a cooperating manner in a benign environment.
- Procedures exist for granting users authorization for access to specific security levels. It is further assumed the TOE administrators will be cleared to the highest security level processed by the TOE.

6 Documentation

The following documentation was used as evidence for the evaluation of the IDS:

6.1 Configuration Management

1. IBM IDS Server Version 11.5 Configuration Management Plan, Revision 0.3, June 12, 2008

6.2 Delivery and Operation

1. IBM IDS 11.50 Delivery Procedures, Revision 0.2, February 4, 2008
2. IBM IDS 11.50 Common Criteria Certification: Requirements for Informix Dynamic Server

6.3 Design Documentation

1. IBM Corporation Informix Dynamic Server Version 11.5 Functional Specification, Revision 0.5, July 11, 2008
2. IBM Corporation Informix Dynamic Server Version 11.5 High Level Design, Revision 0.31, June 10, 2008

3. IBM Corporation Informix Dynamic Server Version 11.5 Low Level Design, Revision 0.4, June 10, 2008
4. IBM Corporation IDS 11.5 Security Policy Model, Revision 0.2, June 2, 2008
5. IBM Informix Dynamic Server source code

6.4 Guidance Documentation

1. IBM IDS 11.50 Common Criteria Certification: Requirements for Informix Dynamic Server
2. IBM Informix, Version 11.50, IBM Informix Dynamic Server Administrator's Guide, 2008
3. IBM Informix, Version 11.50, IBM Informix Security Guide, 2008
4. IBM Informix, Version 11.50, IBM Informix Guide to SQL: Syntax, 2008

6.5 Life Cycle

1. IBM IDS SERVER 11.10 5 for Linux, UNIX, and Windows Life Cycle Document, Revision 0.30, June 13, 2008

6.6 Testing

1. IBM IDS Version 11.5 For Linux, Unix, and Windows Test Plan, Version 0.5, September 25, 2008
2. IBM Corporation Informix Dynamic Server Version 11.5 Test Description, Revision 0.5, September 25, 2008
3. IBM Corporation Informix Dynamic Server Version 11.5 Test Instruction, Revision 0.5, November 21, 2008
4. IBM Corporation Informix Dynamic Server Version 11.5 Identification and Authentication Test, Revision 0.4, November 21, 2008
5. Test code
6. Test Results

6.7 Vulnerability Assessment

1. IBM Informix Dynamic Server (IDS) Enterprise Edition Vulnerability Assessment, Version 0.2, July 17, 2008
2. IBM Informix Dynamic Server (IDS) Enterprise Edition Misuse Analysis, Version 0.2, September 29, 2008

7 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the Evaluation Team Test Report for the IBM IDS, Version 1.0, January 4, 2009.

7.1 Developer Testing

At EAL4, testing must demonstrate correspondence between the tests and the functional specification and high level design. The vendor testing was extensive and covered all of the security functions identified in the ST and interfaces in the design. These security functions include:

- Audit
- Identification and Authentication
- User Data Protection
- Security Management
- Protection of the TSF

7.2 Evaluation Team Independent Testing

The evaluation team installed the product according to the Evaluated Configuration Guide, reran all developer tests and verified the result, then developed and performed functional and vulnerability testing that augmented the vendor testing by exercising different aspects of the security functionality.

As part of its test analysis, the evaluation team analyzed the external protocol interfaces – SQLI and DRDA. For the most part all the security is realized by the SQL verbs within the messages and all the SQL verbs are tested appropriately for access control, audit, and management. The protocol specific testing that is interesting to security is the connection establishment. For both SQLI and DRDA, testing is performed to ensure that connections can only be established with users that have correct username and password combinations. After the connection has been established, all security policies are applied to the SQL requests within the packets. SQLI is used for the SQL verb testing. IBM has argued and the evaluation team has agreed that repeating testing using DRBA is not necessary since the protocol is simply a transport and not security relevant with respect to security checks

8 Evaluated Configuration

The evaluated configuration, as defined in the Security Target, is IBM Informix Dynamic Server version 11.5 (Enterprise Editions) running on any of the following platforms:

Version	Platform	Processor Model	OS Build
Sun 32-bit	Solaris	Sparc	Solaris 9, Solaris10
Sun 64-bit	Solaris	Sparc	Solaris 9, Solaris10
Sun 64-bit	Solaris	AMD64 (Opteron)	Solaris 10
HP 32-bit	HP-UX	PA-RISC	HP-UX 11i, HP-UX 11.23PI, 11.31
HP 64-bit	HP-UX	PA-RISC	HP-UX 11i, HP-UX 11.23PI,11.31
HP 64-bit	HP-UX	Itanium	HP-UX 11.23PI, HP-UX 11.31
HP 32-bit	HP-UX	Itanium	HP-UX 11.23PI, HP-UX11.31
IBM 32-bit	AIX	PowerPC	AIX 5L 5.3
IBM 64-bit	AIX	PowerPC	AIX 5L 5.3

Version	Platform	Processor Model	OS Build
Windows	Windows	x86	Windows 2003, Windows XP,Vista
Intel 32-bit	Linux	x86	RHEL 4, SUSE SLES 10, Asianux 2.05
Intel/AMD 32-bit	Linux	x86_64 (EM64T/AMD64)	RHEL 4, SUSE SLES 10, Asianux 2.05
Intel/AMD 64-bit	Linux	x86_64 (EM64T/AMD64)	RHEL 4, SUSE SLES 10, Asianux 2.05
IBM 64-bit	Linux	PowerPC (pSeries/iSeries, OpenPower, JS20 Blades)	RHEL 4, SUSE SLES 10, Asianux 2.05
IBM 64-bit	Linux	zSeries	RHEL 4, SUSE SLES 10
Intel 64-bit	Linux	Itanium	RHEL 4, SUSE SLES 10
Solaris Opteron 32 bit client only	Solaris	Opteron	

To use the product in the evaluated configuration, the product must be configured as specified in the **IBM Informix Common Criteria Certification: Requirements for Informix Dynamic Server** document.

9 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary ETR. The reader of this document can assume that all EAL4 augmented with ALC_FLR.2 work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 2.3] and CEM version 1.0 [5], [6]. The evaluation determined the IBM IDS TOE to be Part 2 conformant, and to meet the Part 3 Evaluation Assurance Level (EAL 4) augmented with ALC_FLR.2 requirements.

The following evaluation results are extracted from the non-proprietary Evaluation Technical Report provided by the CCTL.

9.1 Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the IDS product that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

9.2 Evaluation of the Configuration Management Capabilities (ACM)

The evaluation team applied each EAL 4 ACM CEM work unit. The ACM evaluation ensured the TOE is identified such that the consumer is able to identify the evaluated TOE. The evaluation team ensured the adequacy of the procedures used by the developer to

accept, control and track changes made to the TOE implementation, design documentation, test documentation, user and administrator guidance, security flaws and the CM documentation. The evaluation team ensured the procedure included automated support to control and track changes to the implementation representation. The procedures reduce the risk that security flaws exist in the TOE implementation or TOE documentation. To support the ACM evaluation, the evaluation team received Configuration Management (CM) records from IBM and performed a CM audit.

9.3 Evaluation of the Delivery and Operation Documents (ADO)

The evaluation team applied each EAL 4 ADO CEM work unit. The ADO evaluation ensured the adequacy of the procedures to deliver, install, and configure the TOE securely. The evaluation team ensured the procedures addressed the detection of modification, the discrepancy between the developer master copy and the version received, and the detection of attempts to masquerade as the developer. The evaluation team followed the Configuration Guide to test the installation procedures to ensure the procedures result in the evaluated configuration.

9.4 Evaluation of the Development (ADV)

The evaluation team applied each EAL 4 ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification, a high-level design document, a low-level design document, and a security policy model. The evaluation team also ensured that the correspondence analysis between the design abstractions correctly demonstrated that the lower abstraction was a correct and complete representation of the higher abstraction.

Additionally, the evaluation team ensured that the security policy model document clearly describes the security policy rules that were found to be consistent with the design documentation.

9.5 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each EAL 4 AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. Both of these guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

9.6 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each EAL 4 ALC CEM work unit. The evaluation team ensured the adequacy of the developer procedures to protect the TOE and the TOE documentation during TOE development and maintenance to reduce the risk of the introduction of TOE exploitable vulnerabilities during TOE development and maintenance. The evaluation team ensured the procedures described the life-cycle model and tools used to develop and maintain the TOE.

In addition to the EAL 4 ALC CEM work units, the evaluation team applied the ALC_FLR.2 work units from the CEM supplement. The flaw remediation procedures were evaluated to ensure that flaw reporting procedures exist for managing flaws discovered in the TOE.

9.7 Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team applied each EAL 4 ATE CEM work unit. The evaluation team ensured that the TOE performed as described in the design documentation and demonstrated that the TOE enforces the TOE security functional requirements. Specifically, the evaluation team ensured that the vendor test documentation sufficiently addresses the security functions as described in the functional specification and high level design specification. The evaluation team performed a sample of the vendor test suite, and devised an independent set of team test and penetration tests. The vendor tests, team tests, and penetration tests substantiated the security functional requirements in the ST.

9.8 Vulnerability Assessment Activity (AVA)

The evaluation team applied each EAL 4 AVA CEM work unit. The evaluation team ensured that the TOE does not contain exploitable flaws or weaknesses in the TOE based upon the developer strength of function analysis, the developer vulnerability analysis, the developer misuse analysis, and the evaluation team's misuse analysis and vulnerability analysis, and the evaluation team's performance of penetration tests.

9.9 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's performance of the entire vendor tests suite, the independent tests, and the penetration test also demonstrated the accuracy of the claims in the ST.

10 Validator Comments/Recommendations

All Validator concerns with respect to the evaluation have been addressed. No issues are outstanding.

11 Annexes

Not applicable.

12 Security Target

The Security Target is identified as *IBM Informix Dynamic Server Version 11.5 Security Target,* Version 1.0, September 25, 2008.

13 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL)**. An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance**. The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation**. The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence**. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE)**. A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation**. The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body**. A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

14 Bibliography

The Validation Team used the following documents to produce this Validation Report:

[1] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model*, Version 2.3, August 2005.

[2] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements,* Version 2.3, August 2005.

[3] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements,* Version 2.3, August 2005.

[4] Common Criteria Project Sponsoring Organisations. *Common Evaluation Methodology for Information Technology Security* – Part 1: Introduction and general model, Version 0.6, 11 January 1997.

[5] Common Criteria Project Sponsoring Organisations. *Common Evaluation Methodology for Information Technology Security* – Part 2: Evaluation Methodology, Version 1.0, August 1999.

[6] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, *Guidance to Validators of IT Security Evaluations,* Scheme Publication #3, Version 1.0, January 2002.

[7] Science Applications International Corporation. *Evaluation Technical Report for the IBM Informix Dynamic Server Version 11.5 Part 2 (Proprietary),* Version 3.0, January 5, 2009.

[8] Science Applications International Corporation. *Evaluation Technical Report for the IBM Informix Dynamic Server Version 11.5 Part 1 (Non-Proprietary),* Version 1.0, December 19, 2008.

[9] Science Applications International Corporation. *Evaluation Team Test Report for the IBM Informix, ETR Part 2 Supplement (SAIC and IBM Proprietary),* Version 1.0, January 4, 2009.

Note: This document was used only to develop summary information regarding the testing performed by the CCTL.

[10] *IBM Informix Dynamic Server Version 11.5 Security Target, Version 1.0, September 25, 2008*