National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

Teradata Database Version 12.0

Report Number: **CCEVS-VR-VID10328-2009**
Dated: **21 August 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

Mike Allen (Lead Validator)
Jandria Alexander (Senior Validator)
Aerospace Corporation
Columbia, Maryland

Common Criteria Testing Laboratory

Science Applications International Corporation (SAIC)
7125 Columbia Gateway Drive, Suite 300
Columbia, Maryland 21046

Table of Contents

1 Executive Summary

This report is intended to assist the end-user of this product and any security certification Agent for the end-user with determining the suitability of this Information Technology (IT) product in their environment. End-users should review both the Security Target (ST), which is where specific security claims are made, in conjunction with this Validation Report (VR), which describes how those security claims were evaluated and any restrictions on the evaluated configuration. Prospective users should carefully read the Validator Comments in Section 10.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Teradata Database Version 12.0. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This Validation Report applies only to the specific version and configuration of the product as evaluated and documented in the Security Target.

The evaluation of the Teradata Database Version 12.0 was performed by Science Applications International Corporation (SAIC), the Common Criteria Testing Laboratory, in Columbia, Maryland USA and was completed in July 2009.

The information in this report is largely derived from the Security Target (ST), Evaluation Technical Report (ETR) and associated test report. The ST was written by Teradata Corporation. The ETR and test report used in developing this validation report were written by SAIC. The evaluation was performed to conform to the requirements of the Common Criteria for Information Technology Security Evaluation, Version 3.1, dated September 2007 at Evaluation Assurance Level 4 (EAL 4) augmented with ALC_FLR.3 and the Common Evaluation Methodology for IT Security Evaluation (CEM), Version 3.1, dated September 2007. The product, when configured as specified in the installation guides and user guides, satisfies all of the security functional requirements stated in the Teradata Database Version 12.0 Security Target. The evaluation team determined the product to be both Part 2 Conformant and Part 3 Augmented, and meets the assurance requirements of EAL 4 with ALC_FLR.3. All security functional requirements are derived from Part 2 of the Common Criteria.

The TOE is a relational database management system (RDBMS) that is designed to access, store, and operate on data using Teradata Structured Query Language (Teradata SQL), which is compatible to ANSI SQL with extensions. The database was developed to allow users to view and manage large amounts of data as a collection of related tables. The database executes as a trusted parallel application (TPA) on a symmetric multiprocessing (SMP) or massively parallel processing (MPP) database server running a commercially available operating system.

During this evaluation, the Validators monitored the activities of the SAIC evaluation team, provided guidance on technical issues and evaluation processes, reviewed successive versions of the Security Target, reviewed selected evaluation evidence, reviewed test plans, reviewed intermediate evaluation results (i.e., the CEM work units), and reviewed successive versions of the ETR and test reports. The Validators determined that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements defined in the Security Target (ST). Therefore, the Validators conclude that the SAIC findings are accurate, the conclusions justified, and the conformance claims correct.

2 Identification

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

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology (IT) 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 (if any); and
- 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
Target of Evaluation	Teradata Database, Version 12.0
Protection Profile	None
Security Target	*Teradata Database Version 12.0 Security Target,* Version 1.7, August, 2009
Dates of evaluation	November 20, 2008 through August 2009
Evaluation Technical Report	*Evaluation Technical Report For the Teradata Database Part 1 (Non-Proprietary),* Version 1.0, July 1, 2009 and *Evaluation Technical Report For the Teradata Database Part 2 (SAIC and Teradata Proprietary),* Version 1.0, July 1, 2009
Conformance Result	Part 2 conformant and EAL4 Part 3 augmented with ALC_FLR.3
Common Criteria version	Common Criteria for Information Technology Security Evaluation Version 3.1R2, September 2007 and all applicable NIAP and International Interpretations effective on November 20, 2008
Common Evaluation Methodology (CEM) version	CEM version 3.1R2 dated September 2007and all applicable NIAP and International Interpretations effective on October 30, 2008
Sponsor	Teradata Corporation, 2835 Miami Village Drive, Miamisburg, Ohio 45342
Developer	Teradata Corporation, 2835 Miami Village Drive, Miamisburg, Ohio 45342
Common Criteria Testing Lab	Science Applications International Corporation (SAIC), Columbia, MD
Evaluators	Tammy Compton, Dawn Campbell and Katie Sykes of SAIC
Validation Team	Jandria Alexander and Mike Allen of The Aerospace Corporation and Michelle Brinkmeyer and Monique Funderburk of the National Security Agency

3 Security Policy

The security requirements enforced by the Teradata Database TOE were designed based on the following overarching security policies:

- **Accountability**. The users of the system shall be held accountable for their actions within the system.

- **Secadmin**. The TOE shall be configured with an authorized security administrator for secure administration of the TOE. This user shall be separate and distinct from other authorized users.

4 Assumptions and Clarification of Scope

The assumptions in the following paragraphs were made during the evaluation of Teradata Database.

4.1 Personnel Security Assumptions

- The Teradata database administrator is competent and trusted not to abuse his/her privileges.

- Administrators are non-hostile, appropriately trained, and follow all administrator guidance

4.2 Physical Security Assumptions

- Appropriate physical security is provided within the domain for the value of the IT assets protected by the TOE and the value of the stored, processed, and transmitted information.

4.3 Operational Security Assumptions

- There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the database server, other than those services necessary for the operation, administration and support of the database.

4.4 Environmental Assumptions

- The operational environment will provide a separate domain for the TOE’s operations.

- The operational environment will ensure the TSF cannot be bypassed in order to gain access to TOE data.

- The operational environment will provide identification and authentication

- Logon access to the underlying operating system is restricted to authorized administrators only.

- The operational environment is at least as robust as the TOE.

- The operational environment will provide a secure (protected from disclosure, spoofing, and able to detect modification) line of communications between remote users and the TOE.

- The operational environment will provide the TOE with the necessary reliable timestamps.

4.5 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- The assumptions about the underlying operating system mean that to achieve true EAL 4 level of assurance for the complete Teradata System requires the operating system and underlying hardware to be evaluated at or above the EAL 4 level of assurance.
- There can be no other applications or servers running on the operating system or hardware platform used to support the Teradata Database.

5 Architectural Information

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

5.1 TOE Overview

The product type of the Teradata Database (TOE) is a relational database management system (RDBMS). The TOE provides the capability to limit TOE access to authorized users, enforce Discretionary Access Controls on objects under the control of the TOE based on user and/or role authorizations, and to provide user accountability via audit of users' actions.

The Teradata Database is designed to access, store, and operate on data using Teradata Structured Query Language (Teradata SQL), which is compatible to ANSI SQL with extensions. The database was developed to allow users to view and manage data as a collection of related tables. The Teradata Database includes security functionality for parallel database environments supporting multiple concurrent users. The security functionality includes:

- user management - including identification and authentication
- password management controls
- discretionary access control model to enforce access controls on database objects and resources (e.g., databases, users, tables, views, stored procedures and macros)
- a set of access rights
- security roles for management of access rights
- a configurable auditing facility

The Teradata Database functions as a database server in a traditional client/server environment. Access requests are made via the Teradata Tools and Utilities that provide connectivity to the database and submit Teradata SQL statements to the database. For any access to the database through its defined external user interfaces, the database ensures that all security enforcement functions are invoked and succeed before any access request is allowed to proceed.

The Teradata Database operates as a parallel application executing as a set of cooperating processes on an underlying host operating system. The host operating system is not part of the TOE but rather part of the supporting operational environment. The operational environment provides several supporting security mechanisms to prevent compromise of the TOE security functions including:

- authentication and authorization of administrator access to database control utilities and other utilities used to manage system resources and I/O interfaces
- isolation of the TOE Security Functions (TSF) to prevent tampering with TSF components (e.g., the TOE processes managing the database)
- network perimeter controls to restrict network access to the database server to mitigate malicious attacks against the operating system upon which the TOE operates

The Teradata Database, as a software TOE, executes on non-TOE hardware and software systems. The major non-TOE hardware and software systems required for use of the TOE include:

- Symmetric multiprocessing (SMP) server with Intel Xeon EM64T processors (minimum 2.33 GHz.) and minimum 6GB of random access memory (RAM) running SUSE Linux Enterprise Server (SLES) 9, 64-bit version

- Massively parallel processing (MPP) server with Intel Xeon EM64T processors (minimum 2.33 GHz.) and minimum 6GB of random access memory (RAM) per node running SUSE Linux Enterprise Server (SLES) 9, 64-bit version

Note: This evaluation is limited to Teradata Database 12.0 running on SUSE Linux Enterprise Server 9, 64 bit version.

The Teradata Database is the only application executing on the server and underlying operating system. Other server applications, such as web server, e-mail server, domain server, directory server, etc. do not run on a Teradata Database server.

5.2 Physical Scope and Boundary

The TOE itself consists of several software subsystems including the Parallel Database Extension (PDE), Gateway for LAN, Session Controller, Parser and Access Module Processors (AMP). A Session Controller and a Parser subsystem are always configured together in what is called a Parsing Engine (PE) virtual processor.

The PDE subsystem is a software interface layer that operates on top of the host operating system and provides an interface between the other database subsystems and the underlying operating system software. PDE includes a BYNET driver that manages the communication devices that interconnect the hardware nodes on which the server software is resident. It provides a standard interface for inter-process communications across nodes in a multi-node environment. PDE also includes a Console module (CNS) that manages the interface for input and output generated from a Database Window (DBW) on the Console.

The Gateway for LAN subsystem provides the client communications interface to Client applications connected via a network interface. It receives all messages sent from the client to the server. This includes messages containing Teradata SQL statements as well as messages for functions such as connecting and disconnecting sessions, determining the configuration of the server, establishing the security protocols to be used between the client and server, and responding to test messages that determine the health of the server over the LAN. For messages that contain Teradata SQL, the Gateway for LAN checks those messages to ensure that they conform to the specified protocol and forwards them to a Parser subsystem. The Gateway for LAN also receives response messages from the PE subsystems and returns them to the appropriate Client application. The Gateway for LAN also interacts with PDE for memory management and message handling services and for access to underlying operating system services.

A PE virtual processor always includes a Session Controller and a Parser subsystem. The Session Controller processes external requests to establish or terminate a logical connection between the application and the server. It also provides for the recovery of sessions following client or server failures. The Session Controller manages session activities, such as logon, password validation and logoff. The Parser decomposes SQL into relational data management processing steps. It processes external requests containing Teradata SQL by syntactically parsing the statements and generating a set of steps comprising an execution plan for the statements. Other Parser modules then access the generated steps and send them to one or more AMP subsystems for execution. Parser modules also monitor the execution of the steps, handle errors encountered during processing and return the execution results to the Gateway for return to the Client application.

An AMP subsystem physically structures the TOE managed relational data and it processes the steps of an SQL execution plan to access that data. It also manages a set of relational tables containing the description of the user defined data objects. The AMP subsystem provides access to these dictionary tables to Client applications through standard SQL and to other database subsystems as needed and is responsible for the integrity of the relational data structures. The AMP subsystem reads and writes the relational data structures from/to disk storage by making calls to the PDE subsystem which subsequently calls the underlying host operating system to perform the required physical read and write operations.

Other components exist in the Teradata Database environment and interface to the database, but are excluded from the definition of the TOE. These components include:

- The operating system on which the database executes
- The database server node upon which the database software and underlying operating system operates
- The disk storage subsystem and its associated SCSI or Fibre Channel interface
- The Console’s Database Window (DBW) utilities software
- The Teradata Tools and Utilities (Client) applications including the Call Level Interface (CLI) software that processes messages sent to, and received from, the database

The physical boundaries of the TOE are depicted in the Figure 1.

There are two **external** user interfaces to the Teradata Database. The Gateway Message interface receives service requests from Client applications and returns responses to the applications upon completion of a service request. The DBW/Utility interface provides for Console access to executable processes of the PDE subsystem.

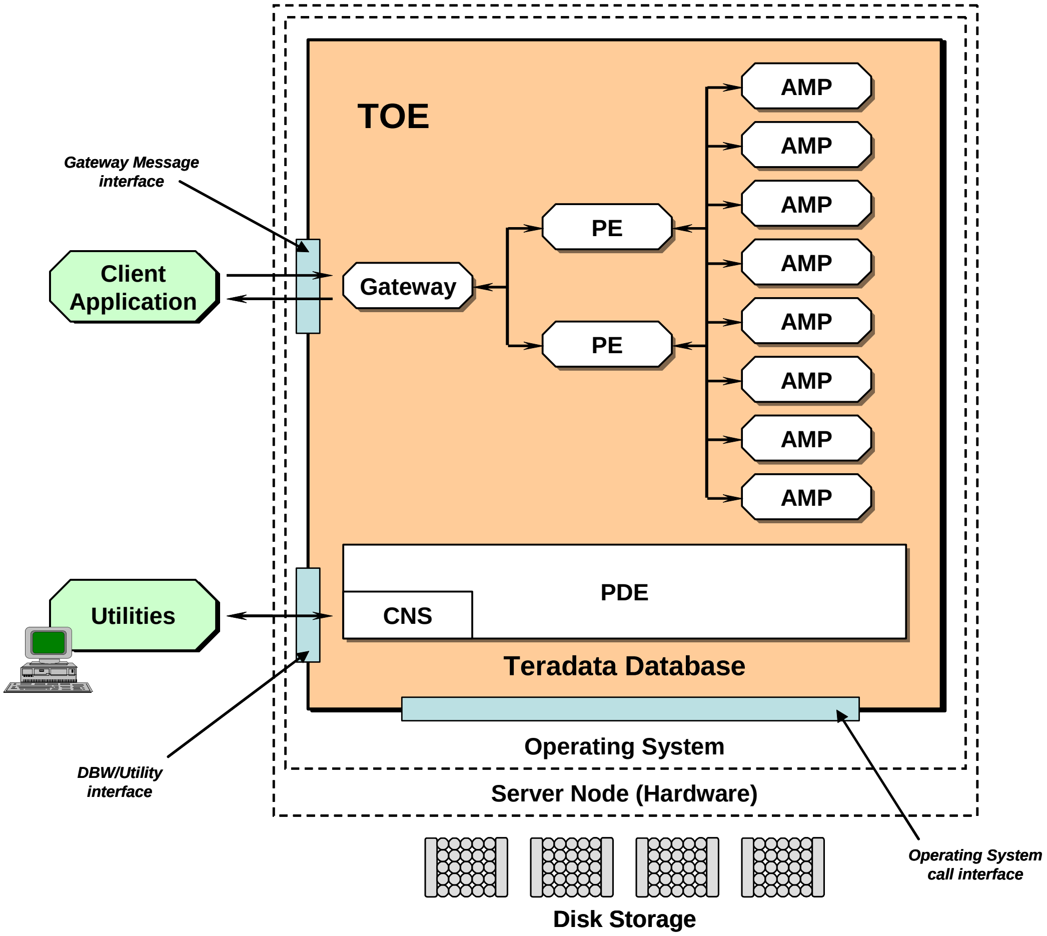

Figure 1: TOE Physical Boundaries

5.2.1 Gateway Message Interface

The Gateway Message interface is the primary external user interface to the Teradata Database. The interface processes text messages which are generated by a client process. Messages are simply a string of character data consisting of a header and a body. The header of a message identifies the kind of message and its length along with other general information. The body consists of data structured for the kind of message defined in the header. The predominant kind of message is one in which the body contains a service request consisting of a SQL statement and associated data. The Gateway Message interface is used to process such service requests from both end users and authorized administrators.

5.2.2 DBW/Utility Interface

The DBW/Utility interface is the external user interface to the Teradata Database PDE subsystem to provide for operational control of the server and for output of operational results of the server's execution. Utilities that use this interface are grouped into the following functional categories:

- Installation, configuration, migration, and upgrade
- System administration and maintenance
- Database administration and operation
- Diagnostics and troubleshooting

Utilities using the DBW/Utility interface do not provide any security functions and do not provide any interface to security functions described in this Security Target.

5.2.3 Operating System Interface

The Teradata Database makes calls to the underlying operating system to access operating system services and to access the associated disk storage subsystem. There is no direct access from the Teradata Database to the underlying hardware - only the operating system accesses the underling hardware.

Note that the TOE is defined as a software-only TOE. As such, the Server Node (Hardware) and Disk Storage is specifically outside the TOE boundary. (The disk storage resides in a separate disk array cabinet that is packaged separately from the Server Node hardware. In some very small environments where the Teradata Database may be running on a standalone server platform, the disk storage may be packaged as part of the server platform.)

The Teradata Database is designed with well-defined interfaces that ensure that all appropriate security checks are made before access is provided to protected database objects and resources. The Teradata Database operates as a set of cooperating processes which are managed by the underlying operating system. These processes operate as a parallel application such that no interference is allowed by processes associated with any non-TOE entities. Furthermore, the Teradata Database is designed such that its interfaces do not allow unauthorized users access to database resources.

Note that given the defined TOE physical boundaries, the TOE protection mechanisms could be bypassed through the underlying operational environment and it is assumed that the operational environment provides appropriate protection mechanisms. The hardware and the operating system upon which the TOE operates both contribute to the enforcement of domain separation between the processes and resources allocated to the TOE and processes and resources that may be allocated to other system functions.

5.3 TOE Logical Boundary

This section identifies the security functions that the TSF provides.

- TOE Access
- User data protection
- Identification and authentication

- Security Audit
- Security management
- Resource Utilization

5.3.1 TOE Access

The Teradata Database allows an authorized security administrator to restrict access to the database based on user identities, *hostid* associated with a network interface, and network (IP) address of the client system.

5.3.2 User Data Protection

The Teradata Database enforces a Discretionary Access Control (DAC) policy for object access based on user identities, object ownership, and active roles. All access to database objects subject to the DAC policy is controlled using access rights. The Teradata Database supports three types of access rights.

- Implicit rights (ownership rights) are implicitly granted to the immediate owner of a database or database object.
- Automatic rights are granted automatically by the system to the creator of a database, user, or object, and to a newly created user or database.
- Explicit rights are granted by any user having the WITH GRANT OPTION privilege for that right.

The database ensures that the requestor has the appropriate access rights before access to a database object is allowed.

Upon initial installation of the Teradata Database, it has only one user. This user is called user DBC and will own all other databases and users in the system. User `DBC` also has access rights on all objects within the database. The administrator guidance recommends that an administrative user be created under user `DBC` and granted access rights for creating and managing other databases and objects. An administrator will log on as that user rather than as user `DBC` to perform normal administrative tasks. Creating an administrative user under user `DBC` is standard practice and provides protection of sensitive data and system objects owned by user `DBC`. Similarly, the administrator guidance also recommends creating a separate security administrator to perform security-related tasks.

5.3.3 Identification and Authentication

The Teradata Database provides user identification and authentication through the use of user accounts and the enforcement of password policies. Users must provide a valid username and password before they can access any database objects or resources. Once identified and authenticated, all subsequent actions allowed within that user's session are based on the user's identity, access rights, and active roles.

Administrator access to database control utilities and other utilities is controlled by a non-TOE component (i.e., the underlying operating system). As such, there is a dependency on the operational environment to provide identification and authentication mechanisms to restrict and control such administrator access.

5.3.4 Security Audit

The Teradata Database automatically audits all successful and failed user logon attempts in the event log. An authorized security administrator may search and sort logon/logoff records using SQL statements to query a defined system view. Additionally, an authorized security administrator may control the monitoring of access rights checks performed by Teradata Database and may search and sort access log records using SQL statements to query a defined system view.

The time stamp used for recording the date and time on which an event is logged is obtained from a non-TOE component (i.e., the underlying operating system). As such, the TOE has a dependency upon the operational environment to provide a reliable time stamp for use by the security audit functions.

5.3.5 Resource Utilization

The Teradata Database enforces maximum quotas and limits on various resources to ensure that those resources are protected from monopolization by any individual database user. Specifically, an authorized security administrator can configure the database to enforce limits on permanent database space allocation, temporary database space usage, and spool database space usage.

5.3.6 Security Management

The Teradata Database provides security management functions that enable an authorized security administrator to manage the secure operation of the database. These functions include management of users, user security attributes, access rights, security roles, and the audit facilities.

6 Documentation

This section provides a complete listing of the IT product documentation provided with the Teradata Database Version 12.0 by the developer to the consumer or available from Teradata on their web site.

Product ID	**Publication Title**
B035-1000-120S	Teradata Database 12.0 Book Set, containing all printed documents shown in this list.
B035-1010-120S	Teradata Database 12.0 Basic Book Set, containing the following books:
B035-1093-067A	Database Administration
B035-1091-067A	Introduction to Teradata Warehouse
B035-1096-067A	Messages
B035-1510-067B	SQL/Data Dictionary Quick Reference
B035-1144-067A	SQL Reference: Data Definition Statements
B035-1146-067A	SQL Reference: Data Manipulation Statements
B035-1143-067A	SQL Reference: Data Types and Literals
B035-1145-067A	SQL Reference: Functions and Operators
B035-1141-067A	SQL Reference: Fundamentals
B035-2401-067A	Teradata Tools and Utilities Command Summary
B035-1511-067B	Utilities Quick Reference
B035-SQLR-120S	SQL Reference Book Set, containing the following books:
B035-1510-067B	SQL/Data Dictionary Quick Reference
B035-1144-067A	SQL Reference: Data Definition Statements
B035-1146-067A	SQL Reference: Data Manipulation Statements
B035-1143-067A	SQL Reference: Data Types and Literals
B035-1145-067A	SQL Reference: Functions and Operators
B035-1141-067A	SQL Reference: Fundamentals
B035-1142-067A	SQL Reference: Statement and Transaction Processing
B035-1148-067A	SQL Reference: Stored Procedures and Embedded SQL
B035-1147-067A	SQL Reference: UDF, UDM, and External Stored Procedure Programming
B035-1092-067A	Data Dictionary
B035-1093-067A	Database Administration
B035-1094-067A	Database Design
B035-1095-067A	Graphical User Interfaces: Database Window and Teradata MultiTool
B035-1091-067A	Introduction to Teradata Warehouse
B035-1096-067A	Messages
B035-1097-067A	Performance Management
B035-1098-067A	Release Summary
B035-1099-067A	Resource Usage Macros and Tables
B035-1100-067A	Security Administration
B035-1510-067B	SQL/Data Dictionary Quick Reference
B035-1144-067A	SQL Reference: Data Definition Statements
B035-1146-067A	SQL Reference: Data Manipulation Statements
B035-1143-067A	SQL Reference: Data Types and Literals
B035-1145-067A	SQL Reference: Functions and Operators
B035-1141-067A	SQL Reference: Fundamentals
B035-1142-067A	SQL Reference: Statement and Transaction Processing
B035-1148-067A	SQL Reference: Stored Procedures and Embedded SQL
B035-1147-067A	SQL Reference: UDF, UDM, and External Stored Procedure Programming
B035-1103-067A	SystemFE Macros
B035-1152-067A	Teradata Replication Solutions Overview

B035-1102-067A	Utilities; Volume 1, A – F; Volume 2, G – S; Volume 3, T - Z
B035-1511-067B	Utilities Quick Reference
B035-1090-067A	Workload Management API: PM/API and Open API
B035-1125-067K	International Character Set Support **(web/CD only)**
B035-1165-067K	ARABIC1256_6A0 to Unicode **(web/CD only)**
B035-1166-067K	CYRILLIC1251_2A0 to Unicode **(web/CD only)**
B035-1135-022K	HANGULEBCDIC933_1II Multibyte to Unicode **(web/CD only)**
B035-1134-022K	HANGULEBCDIC933_1II Single Byte to Unicode **(web/CD only)**
B035-1170-067K	HANGUL949_7R0 Multibyte to Unicode **(web/CD only)**
B035-1169-067K	HANGUL949_7R0 Single Byte to Unicode **(web/CD only)**
B035-1137-022K	HANGULKSC5601_2R4 Multibyte to Unicode **(web/CD only)**
B035-1136-022K	HANGULKSC5601_2R4 Single Byte to Unicode **(web/CD only)**
B035-1164-067K	HEBREW1255_5A0 to Unicode **(web/CD only)**
B035-1061-108K	JIS_COLL Case Blind Collation **(web/CD only)**
B035-1060-108K	JIS_COLL Case-Specific Collation **(web/CD only)**
B035-1175-067K	KANJI932_1S0 Multibyte to Unicode **(web/CD only)**
B035-1174-067K	KANJI932_1S0 Single Byte to Unicode **(web/CD only)**
B035-1055-108K	KanjiEBCDIC Multibyte (Shift-Out/Shift-In) to Unicode **(web/CD only)**
B035-1115-060K	KanjiEUC Code Set 1 to Unicode **(web/CD only)**
B035-1139-122K	KanjiEUC Code Set 2 to Unicode **(web/CD only)**
B035-1116-060K	KanjiEUC Code Set 3 to Unicode **(web/CD only)**
B035-1053-108K	KanjiShiftJIS to KanjiShiftJIS Multibyte **(web/CD only)**
B035-1054-108K	KanjiShiftJIS to Unicode Multibyte **(web/CD only)**
B035-1168-067K	LATIN1250_1A0 to Unicode **(web/CD only)**
B035-1163-067K	LATIN1252_3A0 to Unicode **(web/CD only)**
B035-1171-067K	LATIN1254 to Unicode **(web/CD only)**
B035-1173-067K	LATIN1258_8A0 to Unicode **(web/CD only)**
B035-1050-108K	Multinational Case Blind Default Collation **(web/CD only)**
B035-1062-108K	Multinational Case-Specific Default Collation **(web/CD only)**
B035-1131-022K	SCHEBCDIC935_2IJ Multibyte to Unicode **(web/CD only)**
B035-1130-022K	SCHEBCDIC935_2IJ Single Byte to Unicode **(web/CD only)**
B035-1126-022K	SCHGB2312_1T0 Code Set 0 to Unicode **(web/CD only)**
B035-1127-022K	SCHGB2312_1T0 Code Set 1 to Unicode **(web/CD only)**
B035-1162-067K	SCHINESE936_6R0 Multibyte to Unicode **(web/CD only)**
B035-1161-067K	SCHINESE936_6R0 Single Byte to Unicode **(web/CD only)**
B035-1129-022K	TCHBIG5_1R0 Multibyte to Unicode **(web/CD only)**
B035-1128-022K	TCHBIG5_1R0 Single Byte to Unicode **(web/CD only)**
B035-1133-022K	TCHEBCDIC937_3IB Multibyte to Unicode **(web/CD only)**
B035-1132-022K	TCHEBCDIC937_3IB Single Byte to Unicode **(web/CD only)**
B035-1178-067K	TCHINESE950_8R0 Multibyte to Unicode **(web/CD only)**
B035-1172-067K	TCHINESE950_8R0 Single Byte to Unicode **(web/CD only)**
B035-1167-067K	THAI874_4A0 Single Byte to Unicode **(web/CD only)**
B035-1177-067K	Unicode in Object Names on Japanese Language Support Systems **(web/CD only)**
B035-1176-067K	Unicode in Object Names on Standard Language Support Systems **(web/CD only)**
B035-1104-083K	Unicode to KanjiEBCDIC Multibyte (Shift-Out/Shift-In) **(web/CD only)**
B035-1117-083K	Unicode to KanjiEUC Code Sets 1, 2, and 3 **(web/CD only)**
B035-1058-083K	Unicode to KanjiSJIS Multibyte **(web/CD only)**
B035-1056-036K	Unicode Server Character Set **(web/CD only)**
B035-1057-108K	Unicode to Vargraphic **(web/CD only)**
B035-1725-038K	Release Definition **(web only)**
B035-1909-067D	Teradata User Documentation CD-ROM; Teradata Database 12.0; Teradata Tools and Utilities 12.0 CD-ROM

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 Teradata Database 12.0, Version 1.0, June 26, 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:

- Security Audit
- User Data Protection
- Resource Utilization
- Identification and authentication
- Security management
- TOE Access

7.2 Evaluation Team Independent Testing

The evaluation team verified that the TOE was installed as is specified in the secure installation procedures, reran all developer tests and verified the results, then developed and performed functional and vulnerability testing that augmented the vendor testing by exercising different aspects of the security functionality.

Evaluation team tests were performed in the following areas:

- Independent Tests
  - Confirming that the DBC administrative role has the permissions specified.
  - Testing the ability to revoke a user’s ability to create or access objects.
  - Following the steps in the administrative guidance to ensure that the expected results followed.
  - Verify that no residual information remains when a column is altered.
  - Confirm the password selection rules are enforced.
  - Confirm that the resource utilization constraints are properly enforced.

- Vulnerability Tests
  - Confirmed the database authentication procedures could not be subverted with Linux logon.
  - Port scanning of the TOE in the evaluated configuration to ensure that no ports are open other than those required by the product.

- Testing of the operating system’s discretionary access control settings was performed, and it was determined that the Security Target required an update to ensure that non-administrative personnel were not granted logical access to the system as a result
- Deliberately sending malformed packets over the client server interface to ensure that the server drops the invalid messages.

.

8 Evaluated Configuration

The evaluated configuration, as defined in the Security Target, is Teradata Database Version 12.0 running on SUSE LINUX Enterprise Server 9 (x86_64). The product comes preinstalled in its evaluated configuration as identified in the following manual – Teradata Database Security Administration, Release 12.0, B035-1100-038A.

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 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 and CEM versions 3.1 R2. The evaluation determined the Teradata Database TOE to be Part 2 conformant, and to meet the Part 3 Evaluation Assurance Level (EAL 4) requirements augmented with ALC_FLR.3.

The following evaluation results are extracted from the non-proprietary Evaluation Technical Report provided by the CCTL, and are augmented with the validator's observations thereof.

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 Teradata Database product that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The validators reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.2 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 and a high-level design document. 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.

The validators reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.3 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each EAL4 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.

The validators reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.4 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. The evaluation team re-ran the entire 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.

The validators reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.5 Evaluation of the Life Cycle support Activity (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.3 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.

The validators reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.6 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 evaluation team's vulnerability analysis, and the evaluation team's performance of penetration tests.

The validators reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.7 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 a subset of the vendor tests suite, the independent tests, and the penetration test also demonstrated the accuracy of the claims in the ST.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team followed the procedures defined in the CEM, and correctly verified that the product meets the claims in the ST.

10 Validator Comments/Recommendations

The validation team's observations support the evaluation team's conclusion that the Teradata Database 12.0 meets the claims stated in the Security Target. The validation team also wishes to add the following notations about the use of the product.

- The product must be installed and used in accordance with the guidelines stipulated in the Administrator's Guide to remain in the evaluated configuration.
- There is no restriction provided by the product which prohibits a user or Administrator from specifying a password that would violate DoD 8500 controls guidance, therefore, organizations which use this product must ensure the appropriate controls on password complexity are followed by their users and administrators.
- In a similar manner, the restrictions on failed logon attempts may be bypassed by an Administrator when configuring the system. Administrators must ensure that the appropriate parameter is set to 3.

11 Security Target

The Security Target is identified as the Teradata Database 12.0 Security Target, Version 1.7, August, 2009. The document identifies the security functional requirements (SFRs) that are levied on the TOE, which are necessary to implement the TOE security policies. Additionally, the Security Target specifies the security assurance requirements necessary for EAL 4 augmented with ALC_FLR.3.

12 Glossary

The following abbreviations and definitions are used throughout this document:

CC	Common Criteria
EAL	Evaluation Assurance Level
PP	Protection Profile
SF	Security Functions
SFR	Security Functional Requirement(s)
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy
TSC	TSF Scope of Control

- **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.
- **Threat:** Means through which the ability or intent of a threat agent to adversely affect the primary functionality of the TOE, facility that contains the TOE, or malicious operation directed towards the TOE. A potential violation of security.

- **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.

- **Vulnerabilities:** A vulnerability is a hardware, firmware, or software flaw that leaves an Automated Information System (AIS) open for potential exploitation. A weakness in automated system security procedures, administrative controls, physical layout, internal controls, and so forth, which could be exploited by a threat to gain unauthorized access to information or disrupt critical processing.

13 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 3.1 R2, September 2007.

2.) Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements*, Version 3.1 R2, September 2007.

3.) Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements*, Version 3.1 R2, September 2007.

4.) Common Criteria Project Sponsoring Organisations. *Common Evaluation Methodology for Information Technology Security*, Version 3.1 R2, September 2007.

5.) Common Criteria Project Sponsoring Organisations. *Common Evaluation Methodology for Information Technology Security* – Part 2: Evaluation Methodology, Version 3.1R2, September 2007.

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 Teradata Database Part 2 (Proprietary)*, Version 1.0, July 1, 2009.

8.) Science Applications International Corporation. *Evaluation Team Test Report for the Teradata Database Part 2 Supplement (SAIC and Teradata Proprietary)*, Version 1.0, June 26, 2009.

9.) Teradata Database 12.0 Security Target, Version 1.7, August 2009.