National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme
Validation Report

Science Applications International Corporation
TeraText DBS 4.3.13

Report Number: CCEVS-VR-VID10164-2008
Dated: June 20, 2008
Version: Version 0.2

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 6740
Fort George G. Meade, MD 20755-6740

Table of Contents

Table of figures

1. Executive Summary

This Validation Report (VR) documents the evaluation and validation of the product TeraText DBS 4.3.13, a product of Science Applications International Corporation, Annapolis, MD 21401.

This VR is not an endorsement of the IT product by any agency of the U.S. Government and no warranty of the IT product is either expressed or implied.

The TOE, SAIC TeraText Database System (DBS) 4.3.13 software, is a database server application that is for managing records containing text. The TOE is not a relational database system.

The TOE manages text documents in a variety of formats and encodings including HTML, SGML, XML, RTF, MARC, spreadsheets, word processor documents, plain text, Unicode, and images. It also supports storing images and other non-text formats. For textual data, the TOE provides full text indexing and searching capabilities such as word, field and phrase based querying, fuzzy matching, word stemming, Boolean operators, word distance (proximity) operators, ranking, results sorting, and term highlighting.

The TOE is based on the ANSI Z39.50 protocol, an international standard for distributed search and retrieval. This enables the TOE to scale across multiple servers in order to support large text collections. In this architecture, text is stored in “databases” and databases reside in “content servers”. Databases are somewhat analogous to “tables” in a relational database system. However, one key difference is that Z39.50 enables databases with different physical structures to be accessed as if they have a uniform structure. This is not the case with relational database tables. The TOE also uses a query language that is quite distinct from the Structured Query Language (SQL) used by relational databases.

The TOE can be described in terms of the following components, including the number of instances of each component that are supported in the evaluated configuration:

- TeraText Content Server application (one or more instances)
- TeraText Advanced Search Interface Server application (single instance)
- TeraText Command Line Interface Server application (single instance)
- TeraText APIs (one or more instances)
- TeraText Application Server application (single instance)
- TeraText Database Design Interface Server application (single instance)
- TeraText Security and Logging Server application (single instance)
- TeraText Boot Server application (single instance)
- TeraText Directory Server application (single instance)

The intended environment of the TOE can be described in terms of the following components:

- Operating system
- Web browser
- Java and .NET runtime environments

Aspects of the following security functions are controlled / provided by the TOE in conjunction with its information technology (IT) environment:

- Security audit
- User data protection
- Identification and authentication
- Security management
- Protection of TSF
- TOE access

The evaluation was performed by the CygnaCom Common Criteria Testing Laboratory (CCTL), and was completed during June 2008. The information in this report is derived from the Evaluation Technical Report (ETR) and associated test reports, all written by the CygnaCom CCTL. The evaluation team determined that the product is Common Criteria version 2.2 [CC] Part 2 and Part 3 conformant, and meets the assurance requirements of EAL2 from the Common Methodology for Information Technology Security Evaluation, Version 2.2, [CEM]. The product is not conformant with any published Protection Profiles, but rather is targeted to satisfying specific security objectives.

The evaluation and validation were consistent with National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site www.niap.ccevs.org. The Security Target (ST) is contained within the document SAIC TeraText DBS 4.3.13 Security Target [ST].

2. Identification

Target of Evaluation: SAIC TeraText DBS 4.3.13

Evaluated Software: SAIC TeraText DBS 4.3.13

Developer:

Science Applications International Corporation
1997 Annapolis Exchange Parkway,
Suite 200
Annapolis, Maryland 21401

CCTL:	CygnaCom Solutions Suite 100 West 7925 Jones Branch Drive McLean, VA 22102-3305
Evaluators	Herbert Markle & Kris Rogers, Cygnacom Solutions
Validation Scheme:	National Information Assurance Partnership CCEVS
CC Identification:	Common Criteria for Information Technology Security Evaluation, Version 2.2, January 2004
CEM Identification:	Common Methodology for Information Technology Security Evaluation, Version 2.2, January 2004

3. Security Policy

The TOE's security policy is expressed in the security functional requirements identified in the section 5.1 in the ST. Potential users of this product should confirm that functionality implemented is suitable to meet the user's requirements. A description of the principle security policies is as follows:

- **Security audit**

The TOE generates audit records which contain date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event. Note that auditable events are associated with the identity of the user based on user identifier.

The auditable events include:

- Start-up and shutdown of the audit function (more specifically, of the TOE);
- Successful requests to perform an operation on an object covered by the SFP;
- Unsuccessful use of the authentication mechanism;
- Unsuccessful use of the user identification mechanism, including the user identity provided;

The TOE writes audit records to text files stored in the IT environment that comprise the audit trail. The operating system in the IT environment is relied on to protect audit trail files and for the time. The TOE does not provide any interfaces to read from the audit trail.

- **User data protection**

The TOE can restrict access to Z39.50 databases, records, and schema elements to users and groups based on permissions.

- **Identification and authentication**

The TOE ensures users are identified and authenticated prior to allowing them the ability to access the TOE's security functions. Users are identified with a user name and authenticated with a password. Users attributes include: user name, authentication data (password), and group membership. Note that while the product supports additional authentication mechanisms, only username/password is supported in the evaluated configuration.

- **Security management**

The TOE provides administrator console interfaces that can be used by authorized administrators to perform all management functions, including: managing database subjects (including authentication data), database objects, and TOE session establishment IP addresses.

- **Protection of the TSF**

The TOE can ensure that implicit and explicit policies that it enforces are not bypassed by controlling access to its interfaces, including separating client connections between users and the TOE, and between TOE components. The TOE relies on its platform to operate correctly and to prevent unauthorized access to TOE data and stored executables.

- **TOE access**

The TeraText Content Server component of the TOE can restrict user sessions based on the IP address of the originating client connection (where client in this context is defined as TOE components and subcomponents that initiate Z39.50 connections with the TeraText Content Server).

A summary of the SFRs for the TOE and IT environment are included in the following tables.

TOE Security Functional Requirements

Item	SFR ID	SFR Title
1.	FAU_GEN.1	Audit data generation
2.	FAU_GEN.2	User identity association
3.	FDP_ACC.1	Subset access control
4.	FDP_ACF.1	Security attribute based access control
5.	FIA_ATD.1	User attribute definition
6.	FIA_UAU.2	User authentication before any action
7.	FIA_UID.2	User identification before any action
8.	FMT_MSA.1	Management of security attributes
9.	FMT_MSA.3	Static attribute initialization
10.	FMT_MTD.1a	Management of TSF data
11.	FMT_MTD.1b	Management of TSF data
12.	FMT_MTD.1c	Management of TSF data
13.	FMT_REV.1a	Revocation
14.	FMT_REV.1b	Revocation
15.	FMT_SMF.1	Specification of management functions

Item	SFR ID	SFR Title
16.	FMT_SMR.1	Security roles
17.	FPT_RVM.1a	Non-bypassability of the TSP
18.	FPT_SEP.1a	TSF domain separation
19.	FTA_TSE.1	TOE session establishment

IT Environment Security Functional Requirements

No.	SFR ID	SFR Title
1.	FAU_SAR.1	Audit review
2.	FAU_STG.1	Protected audit trail storage
3.	FPT_RVM.1b	Non-bypassability of the TSP
4.	FPT_SEP.1b	TSF domain separation
5.	FPT_STM.1	Reliable time stamps

4. Assumptions and Clarification of Scope

4.1 Usage Assumptions

For secure usage, the operational environment must be managed in accordance with the documentation associated with the following EAL2 assurance requirements.

ADO_DEL.1 Delivery procedures
ADO_IGS.1 Installation, generation, and start-up procedures
AGD_ADM.1 Administrator guidance
AGD_USR.1 User guidance

4.2 Environmental Assumptions

- Authorized administrators are non-hostile, appropriately trained and follow all administrator guidance.
- There are no general-purpose computing capabilities (e.g., compilers or user applications) available on TOE servers, other than those services necessary for the operation, administration and support of the TOE.
- It is assumed that 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.
- It is assumed that the IT environment provides support commensurate with the expectations of the TOE.
- It is assumed that the environment protects network communication media appropriately.

4.3 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:

1. As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance (EAL2 in this case).
2. This evaluation only covers the specific version identified in this document, and not any earlier or later versions released or in process.
3. As with all EAL2 evaluations, this evaluation did not specifically search for, nor seriously attempt to counter, vulnerabilities that were not "obvious" or vulnerabilities to objectives not claimed in the ST. The CEM defines an "obvious" vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
4. The whole SAIC TeraText DBS 4.3.13 software equals the TOE.
5. TOE depends on IT environment for the following:
    a. to provide the capability to protect audit information.
    b. to provide the capability to view audit information, and alert the authorized administrator of identified potential security violations, using tools in the IT environment such as a text editor to review and search the audit trail file.
    c. will be protected from external interference, tampering or unauthorized disclosure .
    d. will provide protection to the TOE and its assets from external interference or tampering..
    e. to provide reliable time stamps.

The ST provides additional information on the assumptions made and the threats countered.

5. Architectural Information

The TOE consists of the following components:

- TeraText DBS Content Server application
- TeraText DBS Advanced Search Interface Server application
- TeraText DBS Command Line Interface Server application
- TeraText DBS APIs
- TeraText DBS Application Server application
- TeraText DBS Database Design Interface Server application
- TeraText DBS Security and Logging Server application
- TeraText DBS Boot Server application

- TeraText DBS Directory Server application

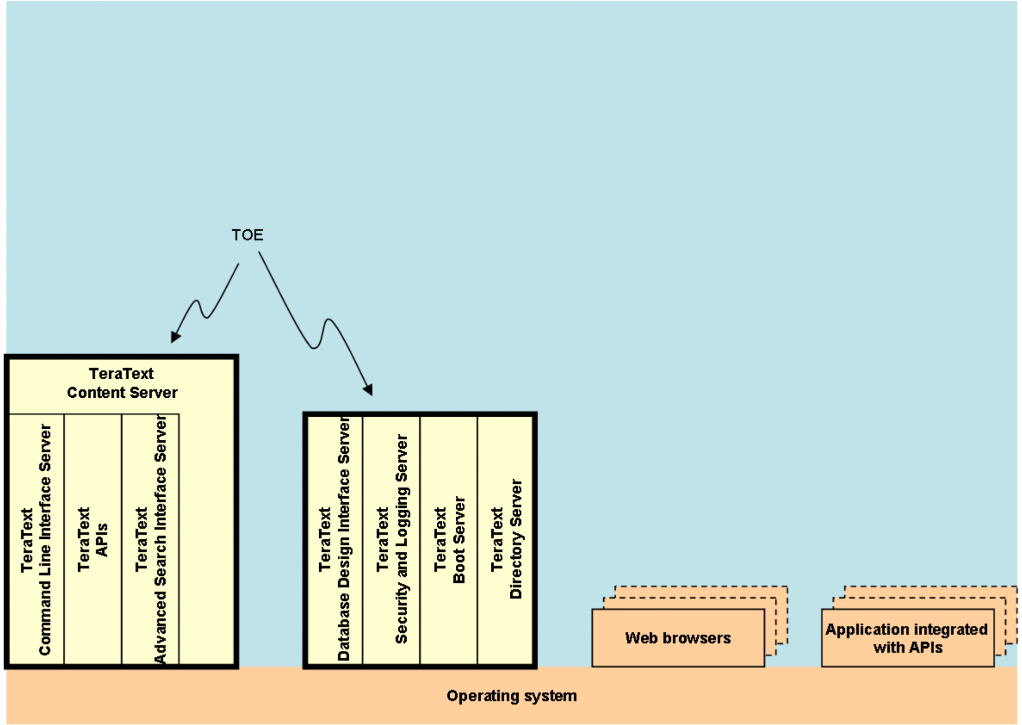
TOE
TeraText Content Server
TeraText Command Line Interface Server
TeraText APIs
TeraText Advanced Search Interface Server
TeraText Database Design Interface Server
TeraText Security and Logging Server
TeraText Boot Server
TeraText Directory Server
Web browsers
Application integrated with APIs
Operating system

Figure 1 - TOE Boundary

6. Documentation

The following is a list of the end-user documentation that was used to support this evaluation:

CC Evaluation Evidence:

- TeraText DBS 4.3.13 Security Target, V1.02, May 22nd, 2008
- TeraText DBS 4.3 CC User's Guide, Revision 5, June 11th, 2008

Product Manuals:

TeraText Database System Release 4.3, Administrator Manual Series:

- Administration Manual, Revision 4.3.0, Nov 9th, 2004
- Application Server Reference Manual, Revision 4.3.0, Nov 9th, 2004
- Application User's Guide, Revision 4.3.0, Nov 9th, 2004
- Boot Server User's Guide, Revision 4.3.0, Nov 9th, 2004
- Common Criteria User's Guide, Revision 5, June 11th, 2008
- Content Server Reference Manual, Revision 4.3.0, Nov 9th, 2004
- Content Server User's Guide, Revision 4.3.0, Nov 9th, 2004

- Database Definition and Modification Reference Manual, Revision 4.3.0, Nov 9th, 2004
- Directory Server User’s Guide, Revision 4.3.0, Nov 9th, 2004
- Getting Started, Revision 4.3.0, Nov 9th, 2004
- Installation Manual, Revision 4.3.0, Nov 9th, 2004
- Security and Logging Server User’s Guide, Revision 4.3.0, Nov 9th, 2004

TeraText Database System Release 4.3, User Manual Series:

- Advanced Search Interface User’s Guide, Revision 4.3.0, Nov 9th, 2004
- Command Line Interface User’s Guide, Revision 4.3.0, Nov 9th, 2004
- Database Design Interface User’s Guide, Revision 4.3.0, Nov 9th, 2004

7. IT Product Testing

At EAL2, the overall purpose of the testing activity is “to determine, by independently testing a subset of the TSF, whether the TSF behaves as specified in the design documentation and in accordance with the TOE security functional requirements specified in the ST” (6.8 [CEM]).

At EAL 2, the developer’s test evidence must only “demonstrate a correspondence between the tests and the functional specification” (ATE_COV.1, Evidence of Coverage [CC]) and does not include a test coverage analysis that shows that the “TSF has been tested against its functional specification in a systematic manner” (ATE_COV.2, Analysis of coverage [CC]). As a result, the developer’s test evidence “need not demonstrate that all security functions have been tested, or that all external interfaces to the TOE Security Function (TSF) have been tested. Such shortcomings are considered by the evaluator during the independent testing sub-activity.” (6.8.2.2 [CEM]).

The objective of the evaluator’s independent testing sub-activity is “to demonstrate that the security functions perform as specified. Evaluator testing includes selecting and repeating a sample of the developer tests” (ATE_IND.2, Independent testing – sample [CC]). The [CEM] provides the general guidance on the various factors that should be considered by the evaluators in devising their test subset and states that the “evaluators should exercise most of the security functional requirements identified in the ST using at least one test” (6.8.4.4 [CEM]). While, the evaluators build on the developer’s testing and use the developer’s correspondence evidence to identify shortcomings in the developer’s test coverage, the evaluators do not perform a test coverage analysis that would demonstrates that all of the security functions as described in the functional specification were tested. As a result, the testing at EAL 2 may not be systematic and the end-users should not assume that all claims in the ST have been explicitly verified by either the developer or the evaluators.

7.1 Developer Testing

The test approach consists of a minimal number of automated tests that run as a group (scripts) or individually (manually). Automated tests are used where testing via APIs is possible and where the results of operations can also be automatically verified.

The test approach in general takes a sampling-based approach, i.e. neither every single combination of parameters for a given interface nor every single interface of a given type are demonstrated. Automated tests generate output indicated if any tests failed to run. Automated tests generate minimal output for tests that pass. The individual scripts perform operations and then verify the results of those operations.

The vendor's testing purposefully (directly) covered the security functions of User data protection, Identification and Authentication, TOE access, as defined in Section 6.1 of the ST. The testing partial covered Security Management (security attributes, attribute initialization, revocation of object attributes, roles). Protection of the TSF was also indirectly supported through the above testing.

The evaluator determined that the developer's approach to testing the TSFs was adequate for an EAL2 evaluation.

7.2 Evaluator Independent Testing

The test approach consists of providing full coverage of all the TOE's security functions between the developer tests and team-defined functional tests as required under EAL 2. The evaluation team performed the following activities during its on-site visit:

1. Installation of the TOE in its evaluation configuration (ADO_IGS.1)
2. Verification of the TOE Installation and configuration (Encompasses all of the below)
3. Execution of the developer's functional tests (ATE_IND.2)
4. Independent Testing (ATE_IND.2)
5. Vulnerability Testing (AVA_VLA.1)
6. All captured output results will be organized in a folder that will be sent with the test report. Filenames that are in *italics* refer to an output file that will be located in a folder called Output Results for Test Report and then under another folder identified by the test name (Test 1) or grouping (audit logs).

The environment and configuration for the Team-Defined testing was the same as that for the Developer Functional testing (see Section 8 of VR).

The independent testing purposefully (directly) covered all the security functions of Security Audit, User data protection, Identification and Authentication, Security Management, TOE access, as defined in Section 6.1 of the ST. Protection of the TSF was also indirectly supported through the above testing and directly supported through vulnerability testing.

All tests passed. No further obvious vulnerabilities were found. However, the evaluation team's independent testing resulted in updates to the Security Target and the CC User's Guide.

The following updates were made to the Security Target:

- Updated access control rules in FDP_ACF.1 and Section 6.1.2 to state that deny access takes priority.
- Updated access control rules in FDP_ACF.1 and Section 6.1.2 to state that users as well as groups can be granted access at the record level.
- Added a note that users also need query permission to perform insert, update, and delete in section 6.1.2
- Clarified that changes to subject attributes do not take effect the next time the user is authenticated, but do take effect before the next access attempt on behalf of the subject. (FMT_REV.1a2)

Additional text was added to Section 3.2 Audit Configuration the CC User's Guide.

7.3 Strength of Function

The TOE depends on the strength of the passwords used to authenticate access by administrative users. For authentication mechanisms a qualification of the security behavior can be made using the results of a quantitative or statistical analysis of the effort required to overcome the mechanism. The overall strength of function (SOF) requirements claim for the TOE is SOF-Basic, which effectively requires resistance to password guessing attacks of greater than one day.

The TOE's SOF analysis assumed that the users will ensure that the passwords are sufficiently random and meet the suggestion of 1 upper case, 1 lower case, 1 special char, and 1 digit with the remaining 4 being any combination of the 94 characters available. The administrator's guidance further recommends that passwords should be complex enough to resist cracking attempts for 1 day at a rate of 1000 guesses per second.

8. Evaluated Configuration

The TOE was installed to its evaluated configuration as shown in Figure 2.

The evaluated configuration includes the following:

SAIC TeraText DBS 4.1.13 was installed on a Sun Platform using the Solaris 8 operating system.

- All TeraText software components will be installed on a Sun Platform using the Solaris 8 operating system.
- A separate Windows XP workstation will be used to access the TeraText Server.

All machines will be installed on a closed network with no connectivity outside the test environment.

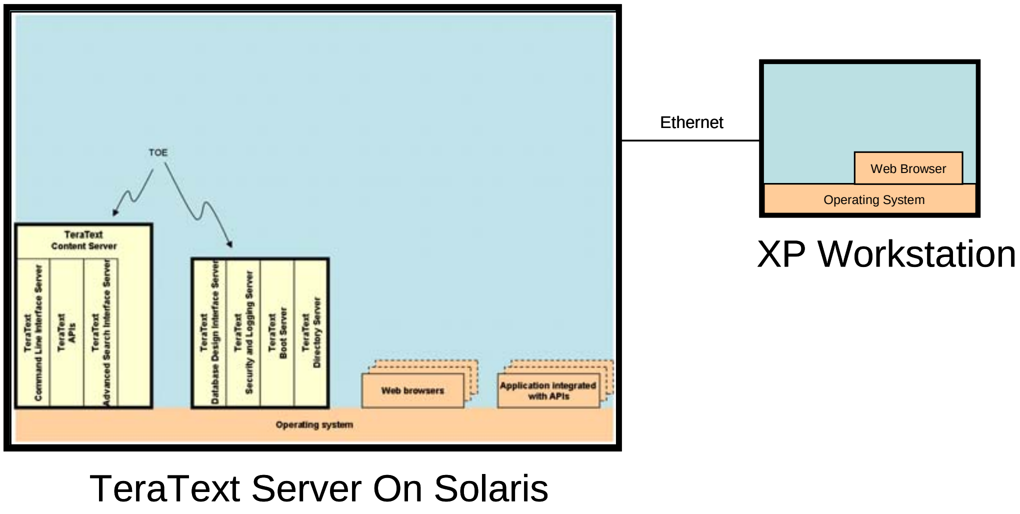
TOE
TeraText Content Server
TeraText Command Line Interface Server
TeraText APIs
TeraText Advanced Search Interface Server
TeraText Database Design Interface Server
TeraText Security and Logging Server
TeraText Boot Server
TeraText Directory Server
Web browsers
Application integrated with APIs
Operating system
TeraText Server On Solaris
Ethernet
Web Browser
Operating System
XP Workstation

Figure 2 - TOE Evaluation Network Configuration

<u>The components that make up the TOE are:</u>

- TeraText Content Server application
- TeraText Advanced Search Interface Server application
- TeraText Command Line Interface Server application
- TeraText APIs
- TeraText Application Server application
- TeraText Database Design Interface Server application
- TeraText Security and Logging Server application
- TeraText Boot Server application
- TeraText Directory Server application

<u>The TOE depends on the following IT Environment Software:</u>

- Operating system – Sun Solaris 8
- Web browser – Internet Explorer 6.0 or more recent, Netscape 6.2 or more recent, Mozilla 1.2 or more recent, Opera 6.03 or more recent.
- Java 1.4.2 and .NET 1.1 runtime environments

- All network node components are out of scope

9. Results of Evaluation

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 version 2.2 of the CC and the CEM.

The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL2 assurance component. For Fail or Inconclusive work unit verdicts, the Evaluation Team advised the developer of issues requiring resolution or clarification within the evaluation evidence. In this way, the Evaluation Team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict.

The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by CygnaCom CCTL. The security assurance requirements are displayed in the following table.

TOE Security Assurance Requirements

Assurance Component ID	**Assurance Component Name**
ACM_CAP.2	CM Documentation
ADO_DEL.1	Delivery procedures
ADO_IGS.1	Installation, generation, and start-up procedures
ADV_FSP.1	Functional specification
ADV_HLD.1	High-level design
ADV_RCR.1	Representation Correspondence
AGD_ADM.1	Administrator guidance
AGD_USR.1	User guidance
ATE_COV.1	Test Coverage Analysis
ATE_FUN.1	Test Documentation
ATE_IND.2	Independent testing
AVA_SOF.1	Strength of TOE Analysis
AVA_VLA.1	Vulnerability analysis

The evaluators concluded that:

The overall evaluation result for the target of evaluation is Pass. The evaluation team reached pass verdicts for all applicable evaluator action elements and consequently all applicable assurance components.

- The TOE is CC Part 2 Conformant
- The TOE is CC Part 3 Conformant for EAL2.
- Strength of Function Rating of SOF-Basic

10. Validator Comments/Recommendations

The Validator's observations support the evaluation team's conclusion that the SAIC TeraText DBS 4.3.1. product meets the claims stated in the Security Target.

- SAIC TeraText DBS 4.3.13 Security Target, Version 1.02, Date May 22, 2008
- SAIC TeraText DBS 4.3.13, Part 1, ETR Version 1.01, Date May 27, 2008
- SAIC TeraText DBS 4.3.13, Part 2, ETR Version 1.01, Date May 27, 2008
- SAIC TeraText DBS V4.3.13, Final Validation Oversight Review Presentation, March 23, 2008

11. Security Target

SAIC TeraText DBS 4.3.13, Security Target Version 1.02 [ST]. The ST is compliant with the Specification of Security Targets requirements found within Annex A of Part 1 of the CC.

12. Glossary

The following table is a glossary of terms used within this validation report.

API	Application Programming Interfact
CC	Common Criteria for Information Technology Security Evaluation
CCEVS	Common Criteria Evaluation and Validation Scheme
CEM	Common Methodology for Information Technology Security Evaluation
CM	Configuration Management
DBA	TeraText DBS Database Administrator
DBS	Database System
EAL	Evaluation Assurance Level
GUI	Graphical User Interface
ID	Identification
IT	Information Technology
JRE	Java Runtime Environment
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
PC	Personal Computer
PP	Protection Profile
SAIC	Science Applications International Corporation
SP	Service Pack
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TSF Interface
TSP	TOE Security Policy

13. Bibliography

URLs

- Common Criteria Evaluation and Validation Scheme (CCEVS): (http://www.niap-ccevs.org/cc-scheme).
- CygnaCom Solutions CCTL (http://www.cygnacom.com).
- SAIC (http://www.saic.com/).

CCEVS Documents

- [CC] Common Criteria for Information Technology Security Evaluation, Version 2.2, January 2004.
- [CEM] Common Methodology for Information Technology Security Evaluation, Version 2.2, January 2004.

Other Documents

- [ST] SAIC TeraText DBS 4.3.13 Security Target, ST Version 1.02, May 22, 2008.