National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

DataPower XS40 XML Security Gateway
and
DataPower XI50 Integration Appliance
Version 3.6

Report Number: **CCEVS-VR-VID10020-2008**
Dated: **30 December 2008**
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

Table of Contents

1. Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of the IBM DataPower XS40 XML Security Gateway and X150 Integration Appliance version 3.6. 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 November 2008. 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 Conformant and Part 3 Conformant**, and meets the assurance requirements of EAL 4 augmented with ALC_FLR.1. The product in its evaluated configuration conforms to U.S. Department of Defense Application-level Firewall Protection Profile (ALFWPP) for Basic Robustness Environments, Version 1.0, June 22, 2000.

The Target of Evaluation (TOE) is the DataPower XS40 XML Security Gateway and the XI50 Integration Appliance, version 3.6 (XS40 and XI50), developed by DataPower Technology, Inc. of Cambridge, MA. DataPower is a wholly-owned subsidiary of IBM. The XS40 and XI50 are network devices that provide Application-Level Firewall functionality. They are hardware enforcement points for Application-Level Firewall policies. The TOE boundary is the hardware appliance and includes the OS and router application software loaded on the appliance. The XS40 and XI50 are separate products, but from the TOE viewpoint are identical when configured in the evaluated configuration.

The evaluated product specification is a subset of the full product capabilities, however, the CCEVS is allowing the product evaluated configuration to be defined as a subset in this case because this evaluation began in 2004, i.e., subsetting of the product was not specifically disallowed in 2004 and so the specification of this product as a subset is being “grandfathered in” in this case. The evaluated configuration is a limited implementation of the products that eliminates any remote administrator access to the TOE by allowing access only through the Serial Port. The firewall is configured to only accept HTTP traffic over TCP/IP and no other traffic is accepted. No other capabilities of the XI50 and XS40 appliances are enabled

The TOE is a special-purpose device that serves as an HTTP-based proxy for one or more backend enterprise services. As such, an important function of the TOE is transformation of an incoming URL into a URL appropriate for the desired backend service and/or transformation of one or more HTTP message header fields. The TOE also provides the typical firewall services of blocking messages from undesired subject addresses, and throttling messages.

The TOE allows administrators to set firewall policies based on

- Presumed address of the source subject
- Presumed address of the destination subject
- Transport layer protocol
- Interface on which traffic arrives and departs
- Service (expressed as a URL)

The TOE also allows administrators to set firewall policies based on HTTP header values (with HTTP considered as an application protocol; TCP is the transport protocol).

The TOE does not allow any information flow through it except under administrative directive. The default policy is "no traffic flow".

The TOE will not accept any malformed (i.e. deviating from specification) messages. All layers in the communications protocol stack are validated for correctness.

Management must be performed locally using a management interface that is included in the Target of Evaluation (TOE).

The 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, reviewed 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) and the U.S. Department of Defense Application-level Firewall Protection Profile (ALFWPP) for Basic Robustness Environments, Version 1.0, June 22, 2000. 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 4 (EAL 4) augmented with ALC_FLR.1 have been met.

The technical information included in this report was obtained from the DataPower XS40 XML Security Gateway and DataPower XI50 Integration Appliance Version 3.6 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.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	DataPower XS40 XML Security Gateway and DataPower XI50 Integration Appliance Version 3.6 (hardware appliances)
Protection Profile	U.S. Department of Defense Application-level Firewall

	Protection Profile (ALFWPP) for Basic Robustness Environments, Version 1.0, June 22, 2000
Security Target	DataPower XS40 XML Security Gateway and DataPower XI50 Integration Appliance Version 3.6 Security Target, Version 0.75, 10/9/2008
Evaluation Technical Report	Final Evaluation Technical Report for DataPower XS40 XML Security Gateway and DataPower XI50 Integration Appliance Version 3.6, Volume I, Version 0.1, 11/19/2008 Final Evaluation Technical Report for DataPower XS40 XML Security Gateway and DataPower XI50 Integration Appliance Version 3.6, Volume II, Version 0.1, 11/19/2008
CC Version	Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 2.3, August 2005. Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 2.3, August 2005. Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements, Version 2.3, August 2005. Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 2.3, August 2005.
Conformance Result	CC Part 2 conformant, CC Part 3 conformant
Sponsor	IBM SOA Appliance Group
Developer	IBM SOA Appliance Group
Common Criteria Test Lab	SAIC, Columbia, MD
CCEVS Validators	Dianne Hale, NIAP Jandria Alexander, Aerospace

3. Architectural Information

The TOE is a hardware appliance with an OS and firewall application software.
The physical boundaries of the TOE consist of the hardware components and the software combination of the Router and the embedded operating system (OS). The Router, a single application, is actually partitioned over two processes. One, the actual Router process, provides the policy-controlled HTTP proxy functionality and administrative operations; the other, called "the watchdog", starts the Router process and ensures that it is running. The watchdog process restarts the Router process in case of a crash. The software combination of the Router process and the OS controls all administrator interaction and all data-flow on- and off-device.
On power-up, the hardware boots the embedded operating system. At the end of its standard startup procedure, the system starts the Router.

Administration is performed using a console connected directly to the TOE's serial port. The administrator uses the TOE's command line interface language (CLI) to administer the TOE. Note that the TOE does not include functionality that would allow for secure remote administration. Remote administration is disallowed in the evaluated configuration.

The TOE subsystems are defined as:

- Hardware — the CPU, persistent data storage, real-time clock, low-level networking (Ethernet)
- Embedded OS — typical operating system facilities: process & memory management, file system, and higher level networking (TCP/IP)
- Router software — application-level firewall functionality as per the ALFWPP

Note that all three subsystems are involved in the main work of the TOE i.e. the processing of network traffic. In relationship to the seven-layer communications model, the Hardware implements the physical and link layers of the communications stack (RJ45 connectors and the Ethernet link protocol); the OS implements the network and transport layers (TCP/IP); and the Router implements the application level protocol (HTTP).

4. Security Policy

The TOE performs the following security functions:

- Security Audit - The TOE records security relevant events associated with individual administrators that occur within its scope of control.
- User Data Protection – The TOE allows authorized administrators and privileged administrators to configure policies that are used to control the flow of network traffic based on a variety of attributes.
- Identification and Authentication (I&A) - The TOE maintains administrator accounts and limits access to only those indentified and authenticated. The TOE also tracks authentication attempts and disables the account after a configured number of failed attempts.
- Security Management - All management functions including defining and modifying administrator accounts including changing an administrator password, setting the time clock, specifying the limits for number of authentication failure attempts, configuring the audit functions are restricted to privileged administrators.
- Protection of the TSF - The TOE provides a security domain for its own execution that prevents untrusted entities from accessing its functions.

5. Assumptions and Clarification of Scope

The evaluated product specification is only a subset of the full product capabilities.The evaluated configuration is a limited implementation of the product that eliminates any remote administrator access to the TOE by allowing access only through the Serial Port. The firewall is configured to only accept HTTP traffic over TCP/IP and no other traffic is accepted. No other capabilities of the XI50 and XS40 appliances are enabled.

The following are assumptions made for the Environment of the TOE:

- Human users within the physically secure boundary protecting the TOE may attempt to access the TOE from some direct connection (e.g., a console port) if the connection is part of the TOE.
- There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.
- The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.
- Privileged and authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.
- Human users who are not authorized administrators can not access the TOE remotely from the internal or external networks.
- The TOE is physically secure.
- The TOE does not host public data.

- Information cannot flow among the internal and external networks unless it passes through the TOE.

6. Documentation

The following documentation is used as evidence for the evaluation of the TOE:

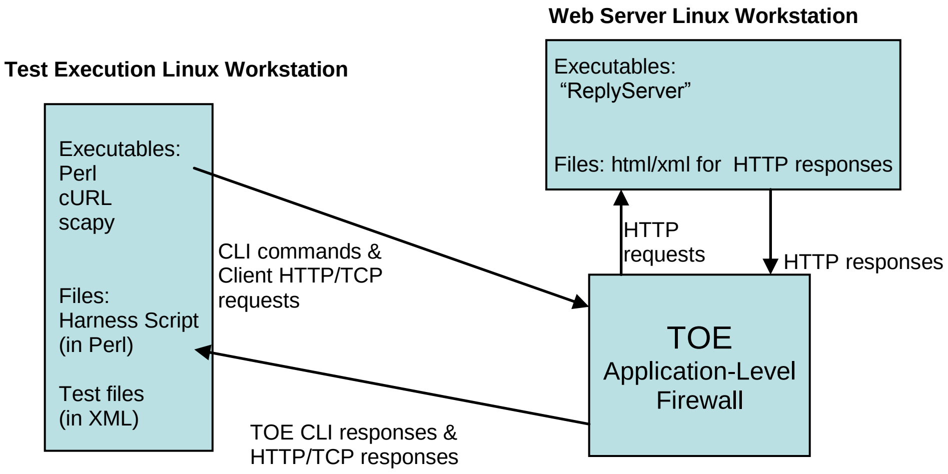
CI Assurance	CI Unique Identifier and description
Analysis of Correspondence (RCR)	DataPower XS40 XML Security Gateway and DataPower XI50 Integration Appliance Version 3.6 Functional Specification, 10/8/2008, Version 13 DataPower XS40 XML Security Gateway and DataPower XI50 Integration Appliance Version 3.6 High Level Design, 10/8/2008, Version 5 DataPower XS40 XML Security Gateway and DataPower XI50 Integration Appliance Version 3.6 Low Level Design, 10/8/2008, Version 4 DataPower XS40 XML Security Gateway and DataPower XI50 Integration Appliance Version 3.6 Security Policy Model, 10/8/2008, Version 5
Analysis of Guidance Documentation (MSU)	DataPower XS40 XML Security Gateway and DataPower XI50 Integration Appliance Version 3.6 Secure Deployment Guide, 10/8/2008, Version 5 Websphere DataPower XS40 XML Security Gateway Reference Guide, Command Reference Guide, Release 3.6.1, December 7, 2007
Configuration Management (ACM)	WebSphere DataPower XS40 XML Security Gateway and WebSphere DataPower XI50 Integration Appliance, Version 3.6, Configuration Management Plan, version 9, 7/21/08
Delivery and Operation (ADO)	WebSphere DataPower XS40 XML Security Gateway and WebSphere DataPower XI50 Integration Appliance Version 3.6 Installation and Delivery Guide, Version 5, March 26, 2007 DataPower XS40 XML Security Gateway and DataPower XI50 Integration Appliance Version 3.6 Secure Deployment Guide, 10/8/2008, Version 5
Functional Specification (FSP)	DataPower XS40 XML Security Gateway and DataPower XI50 Integration Appliance Version 3.6 Functional Specification, 10/8/2008, Version 13
Administration Guide (ADM)	DataPower XS40 XML Security Gateway and DataPower XI50 Integration Appliance Version 3.6 Secure Deployment Guide, 10/8/2008, Version 5 Websphere DataPower XS40 XML Security Gateway Reference Guide, Command Reference Guide, Release 3.6.1, December 7, 2007
Installation Guide (IGS)	DataPower XS40 XML Security Gateway and DataPower XI50 Integration Appliance Version 3.6 Secure Deployment Guide, 10/8/2008, Version 5
User Guide (USR)	Not applicable (all users are administrators)
High-level Design (HLD)	DataPower XS40 XML Security Gateway and DataPower XI50 Integration Appliance Version 3.6 High Level Design, 10/8/2008, Version 5
Life Cycle (ALC)	DataPower XS40 XML Security Gateway Version 3.6 Lifecycle Support, August 4, 2008
Low-level Design (HLD)	DataPower XS40 XML Security Gateway and DataPower XI50 Integration Appliance Version 3.6 Low Level Design, 10/8/2008, Version 4
Security Policy Model (SPM)	DataPower XS40 XML Security Gateway and DataPower XI50 Integration Appliance Version 3.6 Security Policy Model, 10/8/2008, Version 5

CI Assurance	CI Unique Identifier and description
Security Target (ST)	DataPower XS40 XML Security Gateway and DataPower XI50 Integration Appliance Version 3.6 Security Target, Version 0.75, 10/9/2008
Test Documentation (ATE)	WebSphere DataPower XS40 XML Security Gateway and WebSphere DataPower XI50 Integration Appliance Version 3.6 Test Plan, Aug 14, 2008, Version 4
Vulnerability Analysis (VLA)	XS40 XML Security Gateway and XI50 Integration Appliance Version 3.6 Vulnerability Analysis, Version 8, Jan 22, 2007

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 Plan.

The tests were executed on a Linux workstation connected by an ethernet network to the TOE device. The following diagram shows the testing configuration.


Web Server Linux Workstation
Executables:
"ReplyServer"
Files: html/xml for HTTP responses
Test Execution Linux Workstation
Executables:
Perl
cURL
scapy
Files:
Harness Script (in Perl)
Test files (in XML)
CLI commands & Client HTTP/TCP requests
HTTP requests
HTTP responses
TOE
Application-Level Firewall
TOE CLI responses & HTTP/TCP responses

- The developer provided a suite of automated and manual tests that provided both positive and negative tests for all TOE functionality. The evaluator installed both models of the TOE using the vendor's secure deployment guide and then performed all of the vendor tests on both version of the TOE hardware. The test results were exactly those that were expected for both hardware versions of the TOE. There was no difference between the test results based on hardware version.
- The evaluator re-installed the product to ensure that minor changes requested in the secure deployment guide resulted in the expected evaluated configuration
- The evaluator defined and ran the independent tests defined below in addition to the vendor tests:
    - Residual information protection – Tested to ensure that that the packets that are passed

through the firewall are always sized correctly and inappropriately sized packets fail; Verified that all newly allocated objects are initialized.

  - Bug Fix - Performed code review to validate that a vendor identified intermittent bug that affected audit was corrected
  - Stress test for audit log rollover - Demonstrated audit log rollover using stress testing

- The evaluator defined and ran vulnerability and penetration tests defined below:
  - Open source search - Examined open source information to ensure the vulnerability analysis did not miss any well-known vulnerability;
  - Port scan – Performed a port scan to verify that only necessary services are being provided and enabled by the TOE;
  - OS Access – Performed multiple tests to ensure that the Operating System is not accessible to any user;
  - Unapproved commands – Tried all commands included in the documentation and with the "Show" command to ensure that commands not approved for use by a particular user role are inaccessible and that attempts to use them are audited.

No TOE vulnerabilities were identified by the vendor, independent, or penetration tests.

8. Evaluated Configuration

The TOE evaluated configuration consists of the DataPower XS40 XML Security Gateway and DataPower XI50 Integration Appliance Version 3.6 configured as described in the DataPower XS40 XML Security Gateway and DataPower XI50 Integration Appliance Version 3.6 Secure Deployment Guide. **This is a specialized configuration that excludes all product functionality except an application level firewall for HTTP traffic over TCP/IP with administration via a locally connected serial port using the Command Line Interface.**

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, Volume II.

9.1 Evaluation of the Security Target (ST) (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 product that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

9.2 Evaluation of the CM 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.

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.

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.

9.6 Evaluation of the Life Cycle Support Activities (ALC)

he evaluation team applied each EAL 4 ALC CEM work unit, including ALC_FLR.1. 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. The evaluation team ensured that the adequacy of the developer's procedures to track identified flaws and their remediation.

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 security functional requirements are enforced by the TOE. 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 tests 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.

10. Validator Comments / Recommendations

As mentioned throughout this document, the evaluated product specification is only a subset of the full product capabilities . The evaluated configuration excludes all product functionality except an application level firewall for HTTP traffic over TCP/IP with administration via a locally connected serial port using the Command Line Interface. Other product functionality requires independent assessment to verify the functionality as well as to assess the impact on the evaluated functionality.

11. Annexes

Not applicable

12. Security Target

The security target is the DataPower XS40 XML Security Gateway and DataPower XI50 Integration Appliance Version 3.6 Security Target, Version 0.75, 10/9/2008.

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

1. Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 2.3, August 2005.
2. Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 2.3, August 2005.
3. Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements, Version 2.3, August 2005.
4. Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 2.3, August 2005.
5. Final Evaluation Technical Report for DataPower XS40 XML Security Gateway and DataPower XI50 Integration Appliance Version 3.6, Volume II, Version 1.0, 11/19/2008.
6. DataPower XS40 XML Security Gateway and DataPower XI50 Integration Appliance Version 3.6 Security Target, Version 0.75, 10/9/2008.

7. NIAP Common Criteria Evaluation and Validation Scheme for IT Security, Guidance to Common Criteria Testing Laboratories. Version 1.0, March 20, 2001.
8. SAIC CCTL Evaluation Procedures Annex, Version .20, January 31 2004.