National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

U. S. Government Protection Profile~~Department of Defense~~ Directory ~~Protection Profile~~ For Medium Robustness Environments, Version 1.0

Report Number: CCEVS-VR-04-0068
Dated: 17~~8~~ September 2004
Version: ~~0.95~~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 6740
Fort George G. Meade, MD 20755-6740

ACKNOWLEDGEMENTS

Validation Team
Paul Bicknell
The MITRE Corporation
Bedford, MA

Common Criteria Testing Laboratory

Evaluation Team
COACT, Inc
Rivers Ninety Five
9140 Guilford Road, Suite G
Columbia, MD 21046-2587

Table of Contents

1. Executive Summary

The evaluation of *U. S. Department of Defense Directory (DoD) Protection Profile for Medium Robustness Environments*, Version 1.0 was performed by COACT, Inc., a Common Criteria Testing Laboratory (CCTL) in the United States, and was completed on 8 September 2004. The Protection Profile (PP) *U. S. Department of Defense Government Protection Profile (PP) Directory (DoD) Protection Profile (PP) for Medium Robustness Environments* identified in this Validation Report has been evaluated at an accredited testing laboratory using the *Common Methodology for Information TechnologyT Security Evaluation* (Version 1.0) for conformance to the APE requirements of the *Common Criteria for Information Technology Security Evaluation* (Version 2.1). The evaluation was performed by COACT, Inc., a Common Criteria Testing Laboratory (CCTL) in the United States, and was completed on 8 September 2004.

The COACT evaluation team concluded that the Common Criteria requirements for a PP Evaluation have been met.

This Validation Report applies only to the specific version of the PP 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 presented.

The information contained in this Validation Report is not an endorsement of the evaluated PP by any agency of the U. S. Government and no warranty of the PP is either expressed or implied. -

The COACT, Inc., CCTL evaluation team concluded that the Common Criteria requirements for a PP Evaluation have been met.

The technical information included in this report was obtained from *Evaluation Technical Report for the U.S Government t and the Directory Protection Profile for Medium Robustness Environments*, dated September 9, 2004, Document No. F4-0904-001(1), produced by COACT, Inc., CCTL.

1.1 Evaluation Details

Dates of Evaluation: December 2003 through September 2004
Evaluated Product: U. S. Department of Defense Government Protection Profile Directory Protection Profile for Medium Robustness Environments, Version 1.0, dated September 1, 2004
Developer: CygnaCom Solutions, an Entrust Company, and the National Security Agency (NSA),
CCTL: COACT, Inc., Columbia, MD
Validation Team: Paul Bicknell, The MITRE Corporation, Bedford, MA
Evaluation Class: None

PP Conformance: None

1.2 Interpretations

The following interpretations were applied to Common Criteria functional and assurance requirements.

National Interpretations

I-0347	Including Sensitive Information in Audit Records, 2003-07-17
I-0407	Empty Selections Or Assignments, 2003-08-21
I-0410	Auditing of Subject Identity For Unsuccessful Logins, 2002-01-04
I-0414	Site Configurable Prevention of Audit Loss, 2003-07-17
I-0421	Application Notes In Protection Profiles Are Informative Only, 2001-06-22
I-0427	Identification Of Standards, 2001-06-22
I-0429	Selecting One Or More, 2003-08-12

International Interpretations

003	Unique identification of configuration items in the configuration list, 2002-02-11
004	ACM_SCP.*.1C requirements unclear, 2001-11-12
019	Assurance Iterations, 2002-03-11
038	Use of “as a minimum” in C&P elements, 2003-10-31
049	Threats met by environment, 2001-02-16
051	Use of ‘documentation’ without C&P elements, 2002-10-05
056	When can the FPT-RCV dependency be argued away?, 2003-10-31
062	Confusion over source of flaw reports, 2001-07-31
064	Apparent higher standard for explicitly stated requirements, 2001-02-16
080	APE_REQ.1-12 does not use ‘shall examine..to determine’, 2000-10-15
084	Separate objectives for TOE and environment, 2001-02-16
085	SOF Claims additional to the overall claim, 2002-02-11
103	Association of Access Control Attributes with Subjects and Objects, 2003-07-15
111	Settable Failure Limits are Permitted, 2003-10-31
138	Iteration and narrowing of scope, 2002-06-05

1.3 Threats to Security

The Protection Profile identified the following Threats:

Threat	Description of Threat
T. ADMIN_ ERROR	An administrator may incorrectly install or configure the TOE, or install a corrupted TOE, resulting in ineffective security mechanisms.

T.ADMIN_ROGUE	An administrator's intentions may become malicious resulting in user or TSF data being compromised.
T.AUDIT_ COMPROMISE	A malicious user or process may view audit records, cause audit records to be lost or modified, or prevent future audit records from being recorded, thus masking a user's action.
T.CORRUPTED_ IMPLEMENTATION	Unintentional or intentional errors in implementation of the TOE design may occur, leading to flaws that may be exploited by a malicious user or program.
T.CRYPTO_ COMPROMISE	A malicious user or process may cause key, data or executable code associated with the cryptographic functionality to be inappropriately accessed (viewed, modified, or deleted), thus compromise the cryptographic mechanisms and the data protected by those mechanisms.
T.FLAWED_DESIGN	Unintentional or intentional errors in requirements specification or design of the TOE may occur, leading to flaws that may be exploited by a malicious user or program.
T.MALICIOUS_TSF_ COMPROMISE	A malicious user or process may cause TSF data or executable code to be inappropriately accessed (viewed, modified, or deleted).
T.MASQUERADE	A user or process may masquerade as another entity in order to gain unauthorized access to data or TOE resources.
T.POOR_TEST	Lack of or insufficient tests to demonstrate that all TOE security functions operate correctly (including in a fielded TOE) may result in incorrect TOE behavior being discovered thereby causing potential security vulnerabilities.
T.REPLAY	A user may gain inappropriate access to the TOE by replaying authentication information.
T.RESIDUAL_DATA	A user or process may gain unauthorized access to data through reallocation of TOE resources from one user or process to another.
T.RESOURCE_ EXHAUSTION	A malicious process or user may block others from system resources (e.g., CPU time) via a resource exhaustion denial of service attack.
T.SPOOFING	An entity may misrepresent itself as the TOE to obtain authentication data.
T.UNATTENDED_ SESSION	A user may gain unauthorized access to an unattended session.
T.UNAUTHORIZED_A CCESS	A user may gain access to user data for which they are not authorized according to the TOE security policy.
T.UNIDENTIFIED_ ACTIONS	The administrator may fail to notice potential security violations, thus limiting the administrator's ability to identify and take action against a possible security breach.
T.UNKNOWN_ STATE	When the TOE is initially started or restarted after a failure, the security state of the TOE may be unknown.

2. Identification

2.1 PP Identification

PP: *U. S. ~~Department of Defense~~ Government Protection Profile (PP) Directory ~~(DoD) Protection Profile (PP)~~ for Medium Robustness Environments*, Version 1.0, dated September 1, 2004.

CC Identification – *Common Criteria for Information Technology Security Evaluation*, Version 2.11, August August 1999 (CC)1999, ISO/IEC 15408.

CEM Identification – *Common Evaluation Methodology for Information Technology Security Evaluation*, Part 1: Introduction and General Model, Part 2, Version 1.00.6, January August 1999 (CEM)1997.; *Common Methodology for Information Technology Security Evaluation*, Part 2: Evaluation Methodology, Version 1.0, August 1999.

2.2 PP Overview

This PP specifies the minimum-security requirements for Directories (i.e., the Target of Evaluation (TOE)) used by the Department of Defense (DoD) in Medium Robustness Environments. The Directory provides controlled access to a repository of information (RI) for a single classification or marking, and is considered sufficient protection for environments where the likelihood of an attempted compromise is medium. The target robustness level of "medium" is specified in the Guidance and Policy for the Department of Defense Global Information Grid Information Assurance (GIG) [2]. Security Targets (STs) claiming compliance may consist of one or more devices, and, as a medium robustness TOE, must define its TOE to include all the components necessary to meet the security functional requirements, including the hardware.

The PP defines the requirements for a general-purpose Directory that may be used in a variety of applications and systems, including Public Key Infrastructures (PKIs). The TOE for the Directory includes security requirements for identification and authentication (I&A), access control, non-repudiation, audit, trusted channel/path, and TSF management, self-protection, and data availability. A cryptographic module is required for the security mechanisms that use encryption and digital signatures, e.g., trusted channel and I&A, respectively.

Relative to these requirements the PP includes:

- assumptions about the security aspects of the environment in which the TOE will be used;
- threats that are to be addressed by the TOE;
- security objectives of the TOE and its environment;
- functional and assurance requirements to meet those security objectives; and
- rationale demonstrating how the requirements meet the security objectives, and how the security objectives address the threats.

A TOE conformant to the PP satisfies the specified functional requirements, as well as the Medium Robustness assurance requirements that are expressed in the PP. The TOE assurance requirements for the PP are the Medium Robustness Assurance Package and do not map to a CC EAL.

The EAL definitions and assurance requirements in Part 3 of the CC were reviewed and the *Medium Robustness Assurance Package* (refer to *Consistency Instruction Manual For development of Government Protection Profiles (PP) For use in Medium Robustness Environments*) was selected as being best to achieve the goal of addressing circumstances where

developers and users require a moderate to high level of independently assured security in commercial products. The assurance package selection was based on:

- recommendations documented in the GIG;
- DoD Instruction 8500.1; and
- the postulated threat environment.

In order to gain the necessary level of assurance for medium robustness environments explicit requirements have been created for some families. The explicit assurance requirements are summarized in the Table below.

Assurance Class	Assurance Components	
Development	ADV_ARC_EXP.1	Architectural design
	ADV_FSP_EXP.1	Functional Specification with complete summary
	ADV_HLD_EXP.1	Security-enforcing high-level design
	ADV_INT_EXP.1	Modularity decomposition
	ADV_LLD_EXP.1	Security-Enforcing Low-Level design
Vulnerability assessment	AVA_CCA_EXP.2	\Systematic cryptographic module covert channel analysis

2.3 IT Security Environment

The PP includes security requirements associated with a directory server as part of a distributed directory system and as part of a larger system, e.g., a PKI. As a component of these systems the TOE must work in concert with other components to provide system security services. While the PP includes requirements for component security functions to support system security services, it doesn't specify 'how' the requirement must be met. Therefore it does not specify protocols or standards for compliance.

In the PP a distributed directory system is a directory service that resides on more than one directory server. It may partition the repository information among the different servers and it may replicate the repository information among the different servers. A larger system may include a directory as its component, and it may have system-level security requirements that must be supported by its component directory, e.g., system-wide audit data analysis.

3. Security Policy

The Operational Security Policies defined for the TOE are:

Policy	Policy Description
P.ACCESS_BANNER	The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which administrators consent by accessing the system.
P.ACCOUNTABILITY	The authorized users of the TOE shall be held accountable for their actions within the TOE.
P.ADMIN_ACCESS	Administrators shall be able to administer the TOE both locally and remotely through protected communications channels.
P.CRYPTOGRAPHY_ VALIDATED	Where the TOE requires FIPS-approved security functions, only NIST FIPS validated cryptography (methods and implementations) are acceptable for key management (i.e.; generation, access, distribution, destruction, handling, and storage of keys) and cryptographic services (i.e.; encryption, decryption, signature, hashing, key distribution, and random number generation services).
P.CRYPTOGRAPHIC_ FUNCTIONS	The TOE shall provide cryptographic functions for its own use, including encryption/decryption and digital signature operations.
P.NONREPUDIATION	The TOE must provide non-repudiation services for transmitted and received repository data. The non-repudiation services include both the generation and verification of evidence for non-repudiation, including a timestamp, and notification that evidence of receipt the TOE is waiting for is overdue.
P.DISTRIBUTED_DIR ECTORY_SUPPORT	Directories shall be able to support replication. To support replication directories shall be able to replicate (both produce and consume) definable subtrees to other directories (peer trusted directories). Directories shall be able to authenticate using a distributed authentication mechanism.
P.VULNERABILITY_ ANALYSIS_TEST	The TOE must undergo appropriate independent vulnerability analysis and penetration testing to demonstrate that the TOE is resistant to an attacker possessing a medium attack potential.

4. Assumptions

Secure Usage Assumptions

The specific conditions below are assumed to exist in a PP-compliant TOE environment.

Assumption	Assumption Description
A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the IT environment.
A.NO_GENERAL_PURPOSE	There are no general-purpose computing or storage repository capabilities (e.g., compilers, editors, web servers, database servers or user applications) available on the TOE.
A.REMOTE_ADUA_ENVIRONMENT	The accreditation process will ensure that the procuring organization will manage and protect the ADUA in a manner that is commensurate with this PP.
A.REMOTE_ADUA_FUNCTIONALITY	Remote ADUA applications are trusted applications that would comply with the

	security requirements of this PP that are applicable to the ADUA.
A.DISTIRBUTED_DIRECTORY_SECURITY_POLICY_ENFORCEMENT	Before enabling replication and/or distributed I&A mechanisms, the Security Administrator must ensure that the appropriate level of trust has been established and that the I&A and/or access control security policies are understood and enforced.
A.USER_INFORMATION_FLOW	Users will protect all information that is displayed or printed in accordance with both the classification of the data and local security policies.

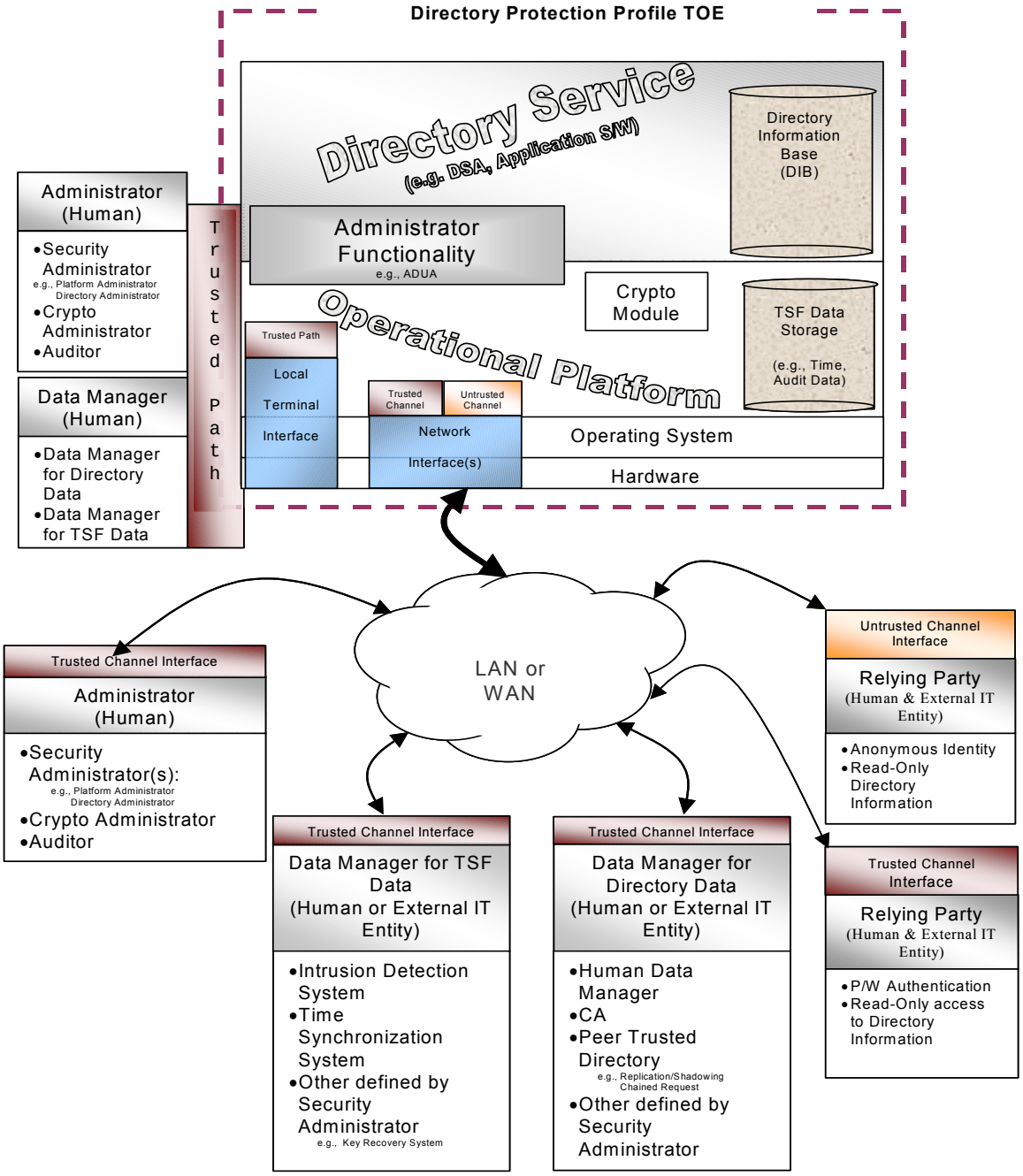
5. Architectural Information

This section describes directory services as the Target of Evaluation (TOE) for the PP.

TOEs claiming conformance to this PP are directories that provide controlled access to a repository of information requiring protection at a Medium Robustness Level of Assurance at a single classification or marking. The PP defines the security requirements for a general-purpose Directory that may be used in a variety of mission critical applications and systems, including PKIs. For example, in a PKI the Directory must ensure certificates and revocation lists are available for relying parties to use certificate-based security mechanisms (e.g., digital signature verification), and it must control access to this security data, e.g., only an authorized Certificate Authority (CA) can update a certain Certificate Revocation List (CRL) entry.

The PP defines the requirements for a Directory which may or may not be a single directory server, but which must be able to function as part of a distributed directory system and as a component of an application system, e.g., PKI. A distributed directory system comprises multiple individual directory servers that interoperate to form an overall distributed directory. Replication and authentication security requirements are included to support this. As a component in a system, e.g., a PKI, the Directory must support system-wide security services. This includes controlled access to audit data for system-wide audit data analysis, and mechanisms to synchronize the Directory's time with other system components.

The architecture, illustrated below, includes all hardware and software components necessary to provide secure directory service. The TOE includes functionality required to administer and manage the Directory both locally and remotely. A trusted local terminal interface (i.e., local console) is included in the TOE. The interface for trusted remote access is not included in the TOE to enable applications to use interfaces appropriate for their system architecture. The TOE does require the remote trusted interfaces establish a trusted channel with the TOE and a trusted path with its users, and that the users authenticate to the TOE.



The functional security requirements included for the Directory, i.e., security services, can be categorized as follows:

- Access Control,
- Identification and Authentication,
- Replication,
- Non-repudiation,
- Audit,
- Trusted Channel/Path,

- Cryptographic Support,
- Administration, and
- Internal Capabilities.

6. Documentation

U. S. Department of Defense (DoD) Government Protection Profile (PP) Directory Protection Profile (PP) for Medium Robustness Environments, Version 1.0, September 1, 2004.

Evaluation Technical Report for U.S Government Directory Protection Profile For Medium Robustness Environments, September 17, 2004, Document No. F4-0904-001(2), produced by COACT, Inc., CCTL.

7. Results of the Evaluation

The Evaluation Team conducted the evaluation in accordance with the APE section of the CC and the CEM.

The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of the APE assurance component. For Fail or Inconclusive work unit verdicts, the Evaluation Team advised the developer of the issue that needed to be resolved or the clarification that needed to be made to the particular evaluation evidence.

The Evaluation Team accomplished this by providing comments inn the draft ETR sections for an evaluation activity (ie.eg., APE) that recorded the Evaluation Team's evaluation results and that the Evaluation Team provided to the developer. The Evaluation Team also constructed Evaluator Observation Reports (EOR) containing descriptions of problems, recommendations, and leaving space for the developer to record their response. The Evaluation Team also communicated with the developer by telephone, electronic mail, and meetings. If applicable, the Evaluation Team re-performed the work unit or units affected. In this way, the Evaluation Team assigned an overall Pass verdict to the APE assurance component only when all of the work units for that component had been assigned a Pass verdict. No constraints or assumptions were identified in performing this evaluation.

Chapter 4, Results of Evaluation, in the Evaluation Team's ETR, states:

"The *U. S. Department of Defense Government Protection Profile Directory Protection Profile for Medium Robustness Environments* was successfully evaluated."

Chapter 5, Conclusions, in the Evaluation Team's ETR, states:

"The *U. S. Government Protection Profile Department of Defense Directory Protection Profile for Medium Robustness Environments* has satisfied the requirements of the *APE Assurance Requirement*s. The PP was assessed against the requirements as stated in the *Common Methodology for Information Technology Security Evaluation. Part 2, Version 1.0.*"

8. Validation Comments/Recommendations

The validation team concurred with the CCTL's evaluation results and had no recommendations concerning the *U.S. Government Protection Profile ~~Department of Defense~~ Directory ~~Protection Profile~~ for Medium Robustness Environments*, Version 1.0.

Comments

Both the PP and the ETR adopted a standardized NIAP interpretation-marking scheme where the labels of CC and CEM requirements and work units were extended to include identification of associated NIAP interpretation. This naming convention can be somewhat complex and difficult to understand but it does ultimately tie each SFR/work-unit to NIAP (and CCIMB) interpretations and allows interpretations coverage to be verified. Without adopting this naming convention it would be very difficult to determine which NIAP and CCIMB interpretations had, in fact, been applied.

This PP represents a very complex architecture that may be difficult for readers to understand without prior knowledge concerning PKI, etc. The fact that directory services can be applied to a whole variety of architectural purposes that are not explicitly mentioned, by example, in the PP may make it difficult for designers of those architectures to identify this PP as being relevant. This PP also presumes a greater, trusted, environment that may need to be "composed" of multiple evaluated products. The issues of assuring security of systems assembled out of evaluated products are numerous and difficult and readers/users of this PP should not assume that doing so is routine.

9. Abbreviations

Abbreviations	Long Form
ADUA	Administrative Directory User Agent
CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Criteria Testing Laboratory
CEM	Common Evaluation Methodology
CPU	Central Processing Unit
CRL	Certificate Revocation List
DoD	Department of Defense
EAL	Evaluation Assurance Level
dmin	Encapsulating Security Patrol
ETR	Evaluation Technical Report
FIPS PUB	Federal Information Processing Standard Publication
GIG	Global Information Grid
IT	Information Technology
I&A	Identification and Authentication
MRE	Medium Robustness Environment

Abbreviations	Long Form
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OR	Observation Report
PKI	Public Key Infrastructure
PP	Protection Profile
RI	Repository of Information
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSE	TOE Security Environment
TSF	TOE Security Function
TSFI	TOE Security Function Interface
TSP	TOE Security Policy
TSS	TOE Summary Specification

10. Bibliography

The evaluation and validation methodology was drawn from the following:

[CC_PART1] Common Criteria for Information Technology Security Evaluation- Part 1: Introduction and general model, dated ~~August~~ August 1999~~1999~~, version 2.1~~1~~.

[CC_PART2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, dated ~~August~~ August 1999~~1999~~, version 2.1~~1~~.

~~[CC_PART2A] Common Criteria for Information Technology Security Evaluation Part 2: Annexes, dated August 1999, version 2.1.~~

[CC_PART3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, dated ~~August~~ August 1999~~1999~~, version 2.1~~1~~.

[CEM~~M_PART 1~~] Common ~~Evaluation~~ Methodology for Information Technology Security Evaluation ~~– Part 1: Introduction and general model~~, Part 2, dated ~~1 November~~ August 1999~~1997~~, version 1.0~~0.6~~.

~~[CEM_PART2] Common Evaluation Methodology for Information Technology Security – Part 2: Evaluation Methodology, dated August 1999, version 1.0.~~

[CCEVS_PUB1] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Organization, Management and Concept of Operations, Scheme Publication #1, Version 2.0 May 1999.

[CCEVS_PUB2] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Validation Body Standard Operating Procedures, Scheme Publication #2, Version 1.5, May 2000.

[CCEVS_PUB3] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Technical Oversight and Validation Procedures, Scheme Publication #3, Version 0.5,

February 2001

[CCEVS_PUB 4] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Guidance to CCEVS Approved Common Criteria Testing Laboratories, Scheme Publication #4, Version 1, March 20, 2001

[CCEVS_PUB 5] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Guidance to Sponsors of IT Security Evaluations, Scheme Publication #5, Version 1.0, August 2000.

[GIG] Department of Defense Chief Information Officer Guidance and Policy Memorandum No. 6-8510, Guidance and Policy for the Department of Defense Global Information Grid Information Assurance (GIG), June 2000.