Australian Government
Department of Defence

Australasian Information Security Evaluation Program

Certification Report

Certificate Number: 2008/49

17 Sep 2008

Version 1.0

Amendment Record

Version	Date	Description
1.0	17/09/2008	Public release.

Executive Summary

1 Microsoft Windows Vista and Windows Server 2008 is the Target of Evaluation (TOE). Microsoft Windows Vista and Windows Server 2008 are pre-emptive multitasking, multiprocessor, and multi-user Operating Systems (OS) that support both workstation and server installations. The OS provides for the application and administration of controlled access to systems and computing resources by users over distributed networks. The following security services included within the TOE Security Functionality (TSF) were evaluated:

a) Security Audit,

b) User Data Protection,

c) Identification and Authentication,

d) Security Management, and

e) TOE Access.

2 This report describes the findings of the IT security evaluation of Microsoft Windows Vista and Windows Server 2008, to the Common Criteria (CC) evaluation assurance level EAL 1. The report concludes that the product has met the target assurance level of EAL 1 and that the evaluation was conducted in accordance with the relevant criteria and the requirements of the Australasian Information Security Evaluation Program (AISEP). The evaluation was performed by **stratsec** and was completed on 8 September 2008.

3 With regard to the secure operation of the TOE, the Australasian Certification Authority (ACA) recommends that:

a) the TOE is only used in its evaluated configuration, ensuring that the security objectives for the supporting environment and assumptions concerning the TOE operational environment, detailed in the Security Target ((ST) Ref [1]), are fulfilled; and

b) the administrator/user configures the TOE according to the Guidance Addendum, found at Appendix B to the ST (Ref [1]).

4 This report includes information about the underlying security policies and architecture of the TOE, and information regarding the conduct of the evaluation.

5 It is the responsibility of the user to ensure that the TOE meets their requirements. For this reason, it is recommended that a prospective user of the TOE refer to the ST (Ref [1]), and read this Certification Report prior to deciding whether to purchase the product.

Table of Contents

CHAPTER 1 - INTRODUCTION 1

1.1 OVERVIEW 1
1.2 PURPOSE 1
1.3 IDENTIFICATION 1

CHAPTER 2 - TARGET OF EVALUATION 3

2.1 OVERVIEW 3
2.2 DESCRIPTION OF THE TOE 3
2.3 SECURITY POLICY 4
2.4 TOE ARCHITECTURE 4
2.4.1 Logical Boundaries 4
2.5 CLARIFICATION OF SCOPE 6
2.5.1 Evaluated Functionality 6
2.5.2 Unevaluated Functionality 7
2.6 USAGE 7
2.6.1 Evaluated Configuration 7
2.6.2 Delivery procedures 8
2.6.3 Determining the Evaluated Configuration 8
2.6.4 Documentation 8
2.6.5 Secure Usage 8

CHAPTER 3 - EVALUATION 9

3.1 OVERVIEW 9
3.2 EVALUATION PROCEDURES 9
3.3 FUNCTIONAL TESTING 9
3.4 PENETRATION TESTING 10

CHAPTER 4 - CERTIFICATION 14

4.1 OVERVIEW 14
4.2 CERTIFICATION RESULT 14
4.3 ASSURANCE LEVEL INFORMATION 14
4.4 RECOMMENDATIONS 14

ANNEX A - REFERENCES AND ABBREVIATIONS 16

A.1 REFERENCES 16
A.2 ABBREVIATIONS 18

Chapter 1 - Introduction

1.1 Overview

6 This chapter contains information about the purpose of this document and how to identify the Target of Evaluation (TOE).

1.2 Purpose

7 The purpose of this Certification Report is to:

a) report the certification of results of the IT security evaluation of the TOE, Microsoft Windows Vista and Windows Server 2008, against the requirements of the Common Criteria (CC) evaluation assurance level EAL 1, and

b) provide a source of detailed security information about the TOE for any interested parties.

8 This report should be read in conjunction with the TOE's ST (Ref [1]) which provides a full description of the security requirements and specifications that were used as the basis of the evaluation.

1.3 Identification

9 Table 1 provides identification details for the evaluation. For details of all components included in the evaluated configuration refer to section 2.6.1 Evaluated Configuration.

Table 1: Identification Information

Item	**Identifier**
Evaluation Scheme	Australasian Information Security Evaluation Program
TOE	Microsoft Windows Vista and Windows Server 2008
Software Versions	This evaluation includes the following: Microsoft Windows Vista Enterprise Edition, Service Pack 1 (32-bit and 64bit versions) Microsoft Windows Server 2008 Standard Edition (32-bit and 64-bit versions) Microsoft Windows Server 2008 Enterprise Edition (32-bit and 64-bit versions) Microsoft Windows Server 2008 DataCentre Edition (64-bit version) Microsoft Windows Server 2008 Itanium Edition (64-bit version)

Item	Identifier
	The following mandatory updates were applied to the TOE (a detailed configuration list is contained in the ST (Ref[1]): MS08-021 KB948590 MS08-025 KB941693 MS08-030 KB951376 MS08-031 KB950759 MS08-032 KB950760 MS08-033 KB951698 MS08-035 KB953235 MS08-036 KB950762
Security Target	Microsoft Windows Vista and Windows Server 2008 EAL1, Version 1.0, 14 August 2008
Evaluation Level	EAL 1
Evaluation Technical Report	Evaluation Technical Report for Microsoft Windows Vista and Windows Server 2008, Version 1.0, 8 September 2008
Criteria	CC Version 3.1, Revision 2, September 2007
Methodology	CEM Version 3.1, Revision 2, September 2007
Conformance	CC Part 2 Conformant CC Part 3 Conformant
Developer	Microsoft Corporation 1 Microsoft Way, Redmond WA 98052-6399 USA
Sponsor	Science Application International Corporation 7125 Columbia Gateway Drive Suite 300, M/S CM6-80 Columbia MD 21046 USA
Evaluation Facility	**stratsec** Suit 1/50 Geils Court, Deakin, ACT 2600

Chapter 2 - Target of Evaluation

2.1 Overview

10 This chapter contains information about the TOE, including: a description of functionality provided; its architecture components; the scope of evaluation; security policies; and its secure usage.

2.2 Description of the TOE

11 The TOE is Microsoft Windows Vista and Windows Server 2008 developed by Microsoft Corporation.

12 Microsoft Windows Vista and Windows Server 2008 are preemptive multitasking, multiprocessor, and multi-user operating systems that support both workstation and server installations. The TOE includes the five software versions of Windows Vista and Windows Server 2008 as listed in Table 1 above and further described as follows:

a) **Microsoft Windows Vista Enterprise** is a client operating system product, suited for business desktop and portable computers (note that portable computers are not included in the evaluated configuration).

b) **Windows Server 2008 Standard** is designed for departmental and standard workloads. It delivers intelligent file and printer sharing; secure connectivity based on Internet technologies, and centralised desktop policy management.

c) **Windows Server 2008 Enterprise** differs from Windows Server 2008 Standard primarily in its support for high-performance servers for greater load handling. These capabilities provide reliability that helps ensure systems remain available.

d) **Windows Server 2008 Datacentre** provides the necessary scalable and reliable foundation to support mission-critical solutions for databases, enterprise resource planning software, high-volume/real-time transaction processing, and server consolidation.

e) **Microsoft Windows Server 2008 for Itanium-Based Systems** provides high levels of performance, reliability, and scalability. It is designed for scalable database workloads and for custom and line-of-business applications.

13 Further details on the TOE and its operating environment are provided in Section 2 of the ST (Ref [1]).

2.3 Security Policy

14 This evaluation was performed at EAL 1. Therefore, no Security Policy Model was provided for the TOE.

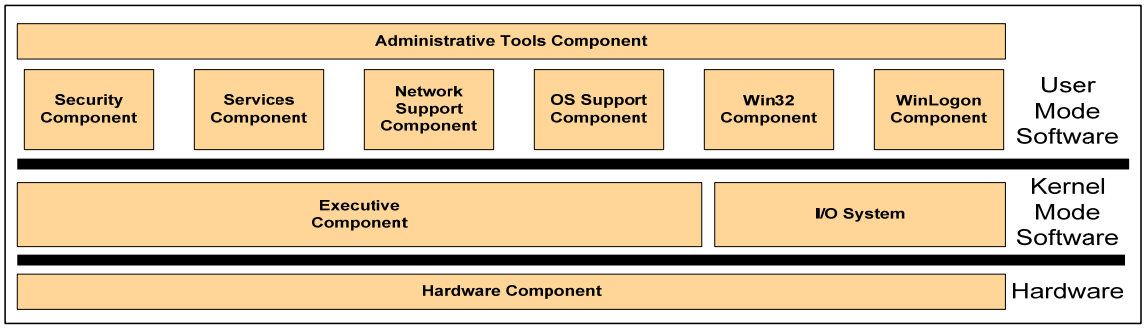
2.4 TOE Architecture

15 Microsoft Windows Vista and Windows Server 2008 include both logical and physical boundaries.

2.4.1 Logical Boundaries

16 The diagram below depicts components and subcomponents of Windows Vista and Windows Server 2008 that comprise the TOE. The components/subcomponents are large portions of the TOE operating systems, and generally fall along process boundaries and a few major subdivisions of the kernel mode software.

Figure 1: TOE Boundaries



17 The system components are:

a) Administrator Tools Module:

i) Administrator Tools Component. This component represents the range of tools available to manage the security properties of the TSF.

b) Hardware Module:

i) Hardware Component. This component includes all hardware used by the TSF to include the processor(s), motherboard and associated chip sets, controllers, and Input/Output (IO) devices.

c) Kernel Software Module:

i) Executive Component. This is the kernel-mode software that provides core OS services to include memory management, process management, and inter-process communication. This

component implements all the non-I/O TSF interfaces for the kernel-mode.

ii) I/O System. This is the kernel-mode software that implements all I/O related services, as well as all driver-related services. The I/O System is further divided into:

(1) I/O Core Component;

(2) I/O File Component;

(3) I/O Network Component; and

(4) I/O Devices Component.

d) Miscellaneous OS Support Module:

i) OS Support Component. This component is a set of processes that provide various other OS support functions and services.

e) Remote Procedure Call (RPC) and Network Support Module:

i) Network Support Component. This component contains various support services for RPC, COM, and other network services.

f) Security Module:

i) Security Component. This component includes all security management services and functions.

g) Services Module:

i) Services Component. This is the component that provides many system services as well as the service controller.

h) Win32 Module:

i) Win32 Component. This component provides various support services for Win32 applications and the command console application.

i) WinLogon Module:

i) WinLogon Component. This component provides various interactive logon services to include interactive authentication, trusted path, session management and locking.

2.4.2 Physical Boundaries

18 Physically, each each TOE workstation or server consists of an x86, x64, or IA64 machine or equivalent processor, with up to four CPUs for a

standard Server product, up to eight CPUs for the Enterprise Server product, and up to 32 CPUs for the Data Centre product. A set of peripheral devices may be attached, including a network adaptor.

19 The TOE does not include any physical network components between network adaptors. The ST assumes that any network connections, equipment, and cables are appropriately protected in the TOE security environment.

2.5 Clarification of Scope

20 The scope of the evaluation was limited to those claims made in the ST (Ref [1]) and includes only the operating system.

2.5.1 Evaluated Functionality

21 The TOE provides the following evaluated security functionality:

a) **Security Audit.** The TOE provides the ability to collect audit data, review audit logs, protect audit logs from overflow, and restrict access to audit logs. Audit information generated by the system includes date and time of the event, user who caused the event to be generated, computer where the event occurred, and other event specific data.

b) **User Data Protection.** The TOE protects user data by enforcing the Discretionary Access Control (DAC) policy and object and subject residual information protection. Windows Vista and Windows Server 2008 use access control methods to allow or deny access to objects, such as files, directory entries, and printers. The TOE also protects user data by ensuring that resources exported to user-mode processes do not have any residual information.

c) **Identification and Authentication.** The TOE requires each user to be identified and authenticated prior to performing any functions. The TOE maintain a database of accounts which includes user identities, authentication information, group associations, privileges and logon rights associations for each security principal. The TOE provides a set of account policy functions that include the ability to define minimum password length, number of failed logon attempts, duration of lockout, and password age.

d) **Security Management.** The TOE includes a number of functions to manage policy implementation. Policy management is controlled through a combination of access control, membership in administrator groups, and privileges.

e) **TOE Access.** The TOE enables a user to lock their session immediately, or after a defined period of inactivity. The TOE constantly monitors input devices for activity and automatically locks the workstation after a defined period of inactivity, if so

configured. The TOE allows an authorised administrator to configure the system to display a logon banner before the logon dialogue is displayed.

2.5.2 Unevaluated Functionality

22 Potential users of the TOE are advised that some functions and services may not have been evaluated as part of the evaluation. Potential users of the TOE should carefully consider their requirements for using functions and services outside of the evaluated configuration. Australian Government users should refer to the Australian Government Information and Communications Technology Security Manual (ACSI 33) (Ref [2]) for policy relating to using an evaluated product in an unevaluated configuration. New Zealand Government users should consult the New Zealand Information and Communications Technology Security Manual (NZSIT 400 Series) (Ref [3]).

23 Microsoft provides software applications, packaged with the operating systems, which are considered outside the scope of the defined TOE and thus not part of the evaluated configuration. Services outside this evaluation include:

a) Internet Information Services,

b) Windows Firewall,

c) Certificate Services,

d) Terminal Services,

e) Microsoft Message Queuing,

f) Rights Management Services, and

g) Windows SharePoint Services.

2.6 Usage

2.6.1 Evaluated Configuration

24 This section describes the configurations of the TOE that were included within scope of the evaluation. The assurance gained via evaluation applies specifically to the TOE in these defined evaluated configuration(s). Australian Government users should refer to ACSI 33 (Ref [2]) to ensure that configuration(s) meet the minimum Australian Government policy requirements. New Zealand Government users should refer to NZSIT 400 Series (Ref [3]).

25 The evaluated configurations are provided in the Guidance Addendum, found at Appendix B to the ST (Ref [1]). The key policies that are applied to the TOE in the evaluated configuration are:

a) Minimum password length and complexity requirements;

b) Access banner configuration; and

c) TOE access history.

26 The guidance also provides recommendations for Auditing. The evaluators noted that the provided guidance (TOE Help files) was limited, and while sufficient, significant additional resources are available on the Internet. The evaluators recommend that administrators of the TOE do additional research to ensure that they are fully aware of the possible TOE uses and configurations.

27 The TOE does not counter the threat of information disclosure by authorised users. Users are explicitly trusted to use the TOE in a secure manner and ensure that the TOE is in the evaluated configuration.

2.6.2 Delivery procedures

28 The TOE delivery procedures are not evaluated at EAL 1. However, the administrator/user can have some assurance that the TOE has not been tampered with if the manufacturers shrink wrapped packaging is intact.

2.6.3 Determining the Evaluated Configuration

29 The TOE is provided on DVD and installation of the TOE is initiated by booting the hardware from the DVD. Once the installation process has commenced, the administrator/user simply follows the on screen instructions, and when completed has a base image of the Operating System to start from. The administrator/user must then configure the TOE according to the Guidance Addendum (Ref [1]).

2.6.4 Documentation

30 It is important that the TOE is used in accordance with the TOE Help files (delivered with the product) and the Guidance Addendum (Ref [1]) in order to ensure its secure usage.

2.6.5 Secure Usage

31 The evaluation of the TOE took into account certain assumptions about its operational environment. The following assumption must hold in order to ensure the security objectives of the TOE are met.

Table 2: Environmental Assumptions

Assumption Identifier	Assumption Description
A.ACCURATE_CLOCK	It is assumed that a reliable hardware clock is provided by the hardware.

Chapter 3 - Evaluation

3.1 Overview

32 This chapter contains information about the procedures used in conducting the evaluation and the testing conducted as part of the evaluation.

3.2 Evaluation Procedures

33 The criteria against which the TOE has been evaluated are contained in the Common Criteria for Information Technology Security Evaluation (Refs [5], [6] & [7]). The methodology used is described in the Common Methodology for Information Technology Security Evaluation (Ref [8]). The evaluation was also carried out in accordance with the operational procedures of the AISEP (Refs [9], [10], [11] and [12]). In addition, the conditions outlined in the Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security (Ref [13]) were also upheld.

3.3 Functional Testing

34 Evaluation of the developer's testing of the TOE is not performed at EAL 1. However, six independent functional tests were developed and performed by the evaluators to verify the TOE functionality.

Table 3: Evaluator Test Summary

Identifier	Description	Security function	Result
IND01	To test that each user is identified and authenticated prior to performing TSF-mediated functions on behalf of that user, regardless of whether the user is logging on interactively, or is accessing the system via a network connection.	FIA_AFL.1 FIA_ATD.1 FIA_SOS.1 FIA_UAU.1 FIA_UAU.6 FIA_UAU.7 FIA_UID.1 FIA_USB.1 FTA_TAB.1 FMT_MTD.1a FTA_TSE.1 FMT_SAE.1 FMT_SMR.1 FMT_MOF.1b FMT_MTD.1c FMT_MTD.1d FMT_MTD.1e FMT_MTD.1f FMT_SMR.1	Pass

Identifier	Description	Security function	Result
IND02	To test the TOE access policies are implemented and applied to the Microsoft Server 2008 and Vista Operating System in both Active Directory and standalone environment.	FTA_SSL.1 FTA_SSL.2 FTA_TAB.1 FTA_TAH.1	Pass
IND03	To test the TOE access policies (based on time, day and location) are implemented and applied to the Microsoft Server 2008 and Vista Operating System.	FTA_TSE.1	Pass
IND04	To the test TSF generates an alarm to the authorized administrator if the audit trail exceeds specified log size.	FAU_STG.3	Pass
IND05	To collect audit data, review audit logs, protect audit logs from overflow, and restrict access to audit logs. Audit information generated by the system includes date and time of the event, user who caused the event to be generated, computer where the event occurred, and other event specific data. Authorised administrators can review audit logs and configure the TOE to only collect events for which the administrator is interested, based on a defined set of criteria.	FPT_STM.1 FAU_GEN.1 FAU_GEN.2 FAU_SAR.1 FAU_SAR.2 FAU_SAR.3 FAU_SEL.1 FAU_STG.1 FMT_MOF.1a FMT_MTD.1b	Pass
IND06	To test the TSF to ensure that it does protect the user data by enforcing access control policy and object and subject residual information protection	FDP_ACC.2 FDP_ACF.1 FMT.MSA.1a FMT_MSA.1b FMT.MSA.3a FMT_REV.1b FDP_RIP.2 FMT_REV.1a FMT_REV.1b	Pass

3.4 Penetration Testing

35 The evaluators performed a vulnerability analysis and penetration testing of the TOE in order to identify any obvious vulnerability in the product, and determined that the TOE is resistant, in its intended environment, to attacks performed by an attacker possessing a basic attack potential. This analysis included a search for possible vulnerabilities available in the following public domain sources:

a) http://secunia.com/, and

b) http://www.securityfocus.com/vulnerabilities.

36 The vulnerabilities identified, and the tests conducted are listed in the following table.

Table 5: Vulnerability Test Summary

Vulnerability	Test / Justification
CVE-2008-0087 This spoofing vulnerability exists in Windows DNS clients and could allow an attacker to send specially crafted responses to DNS requests, thereby spoofing or redirecting Internet traffic from legitimate locations.	Confirm the vulnerability does exist in the TOE. Apply the vendor solution “MS08-020”. Confirm the vulnerability has been fixed.
CVE-2008-1083 / CVE-2008-1087 Exploitation of either of these vulnerabilities could allow remote code execution if a user opens a specially crafted EMF or WMF image file. An attacker who successfully exploited these vulnerabilities could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.	Confirm the vulnerability does exist in the TOE by conducting a vulnerability assessment. Apply the vendor solution “MS08-021”. Confirm the vulnerability has been fixed.
CVE-2008-1086 The vulnerability could allow remote code execution if a user viewed a specially crafted Web page using Internet Explorer. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.	Confirm the vulnerability does exist in the TOE by conducting a vulnerability assessment. Apply the vendor solution “MS08-023”. Confirm the vulnerability has been fixed.
CVE-2008-1085 A remote code execution vulnerability exists in Internet Explorer because of the way that it processes data streams. An attacker could exploit the vulnerability by constructing a specially crafted Web page. When a user views the Web page, the vulnerability could allow remote code execution. An attacker who successfully exploited this vulnerability could gain the same user rights as the logged on user.	Confirm the vulnerability does exist in the TOE by conducting a vulnerability assessment. Apply the vendor solution “MS08-024”. Confirm the vulnerability has been fixed.

Vulnerability	Test / Justification
CVE-2008-1084 An elevation of privilege vulnerability exists due to the Windows kernel improperly validating input passed from user mode to the kernel. The vulnerability could allow an attacker to run code with elevated privileges. An attacker who successfully exploited this vulnerability could execute arbitrary code and take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.	Confirm the vulnerability does exist in the TOE by conducting a vulnerability assessment. Apply the vendor solution “MS08-025”. Confirm the vulnerability has been fixed.
CVE-2008-1453 The vulnerability is caused due to an error in the Bluetooth stack when processing service description requests. This can be exploited by rapidly sending a large number of specially crafted SDP (Service Discovery Protocol) packets to a vulnerable system. Successful exploitation may allow execution of arbitrary code, but requires that Bluetooth is enabled.	Confirm the vulnerability does exist in the TOE by conducting a vulnerability assessment. Apply the vendor solution “MS08-030”. Confirm the vulnerability has been fixed.
CVE-2007-0675 The vulnerability could allow remote code execution if a user viewed a specially crafted Web page using Internet Explorer and has the Speech Recognition feature in Windows enabled. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.	Confirm the vulnerability does exist in the TOE by conducting a vulnerability assessment. Apply the vendor solution “MS08-032”. Confirm the vulnerability has been fixed.

Vulnerability	Test / Justification
CVE-2008-0011 / CVE-2008-1444 An attacker who successfully exploited either of these vulnerabilities could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.	Confirm the vulnerability does exist in the TOE by conducting a vulnerability assessment. Apply the vendor solution "MS08-033". Confirm the vulnerability has been fixed.
CVE-2008-1445 A denial of service vulnerability exists in implementations of Active Directory on Microsoft Windows Server 2008. The vulnerability also exists in implementations of Active Directory Lightweight Directory Services (AD LDS) when installed on Windows Server 2008. The vulnerability is due to insufficient validation of specially crafted LDAP requests. An attacker who successfully exploited this vulnerability could cause the computer to stop responding and automatically restart.	Confirm the vulnerability does exist in the TOE by conducting a vulnerability assessment. Apply the vendor solution "MS08-035". Confirm the vulnerability has been fixed.
CVE-2008-1441 A denial of service vulnerability exists in implementations of the Pragmatic General Multicast (PGM) protocol on Windows Vista, and Windows Server 2008. The protocol's parsing code does not properly validate specially crafted PGM fragments and will cause the affected system to become non-responsive until the attack has ceased.	Confirm the vulnerability does exist in the TOE by conducting a vulnerability assessment. Apply the vendor solution "MS08-036" Confirm the vulnerability has been fixed.
Audit Logs	To test potential vulnerabilities that could affect the operation of the audit function. The tests included the following: a) stopping the audit services, b) deleting the audit log, and c) modifying the audit log.

Chapter 4 - Certification

4.1 Overview

37 This chapter contains information about the result of the certification, an overview of the assurance provided by the level chosen, and recommendations made by the certifiers.

4.2 Certification Result

38 After due consideration of the conduct of the evaluation as witnessed by the certifiers, and of the Evaluation Technical Report (Ref [14]), the Australasian Certification Authority certifies the evaluation of Microsoft Windows Vista and Windows Server 2008 performed by the Australasian Information Security Evaluation Facility (AISEF), **stratsec**.

39 **stratsec** has found that Microsoft Windows Vista and Windows Server 2008 upholds the claims made in the Security Target (Ref [1]) and has met the requirements of the Common Criteria (CC) evaluation assurance level EAL 1.

40 Certification is not a guarantee of freedom from security vulnerabilities.

4.3 Assurance Level Information

41 EAL1 provides a basic level of assurance by a limited ST and an analysis of the security functions in that ST, using a functional and interface specification and guidance documentation, to understand the security behaviour.

42 The analysis is supported by a search for potential vulnerabilities in the public domain and independent testing (functional and penetration) of the TOE security functions.

43 EAL1 also provides assurance through unique identification of the TOE and of the relevant evaluation documents.

44 This EAL provides a meaningful increase in assurance over unevaluated IT.

4.4 Recommendations

45 Not all of the evaluated functionality present in the TOE may be suitable for Australian and New Zealand Government users. For further guidance, Australian Government users should refer to ACSI 33 (Ref [2]) and New Zealand Government users should consult the NZSIT 400 Series (Ref [3]).

46 In regard to the secure operation of the TOE, the ACA recommends that:

a) the TOE is only used in its evaluated configuration, ensuring that the security objectives for the supporting environment and assumptions concerning the TOE operational environment, detailed in the Security Target ((ST) Ref [1]), are fulfilled; and

b) the administrator/user configures the TOE according to the Guidance Addendum, found at Appendix B to the ST (Ref [1]).

47 The ACA also recommends that when deploying Microsoft Vista Enterprise and Windows Server 2008, administrators/users undertake additional web research to ensure that they are fully aware of the possible TOE uses and configurations.

Annex A - References and Abbreviations

A.1 References

[1] Microsoft Windows Vista and Windows Server 2008 EAL1 Security Target, Version 1.0, 14 August 2008.

[2] Australian Government Information and Communications Technology Security Manual (ACSI 33), September 2007, Defence Signals Directorate, (available at www.dsd.gov.au/library/infosec/acsi33.html).

[3] New Zealand Information and Communications Technology Security Manual (NZSIT 400 Series), February 2008, Government Communications Security Bureau (available at www.gcsb.govt.nz/newsroom/nzsits.html).

[4] Windows Vista/Windows Server 2008 EAL1 Evaluation Guidance Addendum, 27 June 2008 (Appendix B to ST (Ref [1])).

[5] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model (CC), Version 3.1, Revision 1, September 2006, CCMB-2006-09-001.

[6] Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components (CC), Version 3.1, Revision 2, September 2007, CCMB-2007-09-002.

[7] Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components (CC), Version 3.1, Revision 2, September 2007, CCMB-2007-09-003.

[8] Common Methodology for Information Technology Security Evaluation, Evaluation methodology, Version 3.1, Revision 2, September 2007, CCMB-2007-09-004.

[9] AISEP Publication No. 1 (AP 1), Program Policy, Version 3.1, 29 September 2006, Defence Signals Directorate.

[10] AISEP Publication No. 2 (AP 2), Certifier Guidance, Version 3.0, 21 February 2006, Defence Signals Directorate.

[11] AISEP Publication No. 3 (AP 3), Evaluator Guidance, Version 3.1, 29 September 2006, Defence Signals Directorate.

[12] AISEP Publication No. 4 (AP 4), Sponsor and Consumer Guidance, Version 3.1, 29 September 2006, Defence Signals Directorate.

[13] Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, May 2000 (available at www.dsd.gov.au/library/pdfdocs/CCDocumentation/ccra.pdf).

[14] Evaluation Technical Report for Microsoft Windows Vista and Windows Server 2008, Version 1.0, 8 September 2008 (EVALUATION-IN-CONFIDENCE).

A.2 Abbreviations

ADLDS	Active Directory Lightweight Directory Services
ACA	Australasian Certification Authority
AISEF	Australasian Information Security Evaluation Facility
AISEP	Australasian Information Security Evaluation Program
CC	Common Criteria
CPU	Central Processing Unit
DAC	Discretionary Access Control
DSD	Defence Signals Directorate
DNS	Domain Naming Service
EAL	Evaluation Assurance Level
EMF	Extended (Enhanced) Windows Metafile Format
ETR	Evaluation Technical Report
GCSB	Government Communications Security Bureau
I/O	Input/Output
LDAP	Lightweight Directory Access Protocol
OS	Operating System
PGM	Pragmatic General Multicast
RPC	Remote Procedure Call
SDP	Service Discovery Protocol
SFP	Security Function Policy
SFR	Security Functional Requirements
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSP	TOE Security Policy
WMF	Windows Metafile