Australian Government
Department of Defence

Australasian Information Security Evaluation Program

Certification Report

Certificate Number: 2010/71

10 Dec 2010

Version 1.0

Amendment Record

Version	Date	Description
1.0	10/12/10	Public release.

Executive Summary

1 The target of evaluation (TOE) is the Xerox WorkCentre 4250 and 4260 Multifunction Systems which consists of a single product with varying feature sets.

2 The TOE is a Multifunction device (MFD) that copies and prints, with scan-to-e-mail, network scan and fax option. The TOE provides an image overwrite package that operates two independent settings. One is the immediate image overwrite setting (IIO). This function forces any temporary image files created on the hard disk drive during a copy, print, network scan or scan-to-email to be overwritten when those files are no longer needed. Alternatively the overwrite process can be performed by an administrator "on demand" known as on-demand image overwrite (ODIO).

3 This report describes the findings of the IT security evaluation of Xerox Corporation's Xerox WorkCentre 4250 and 4260 Multifunction Systems to Common Criteria (CC) evaluation assurance level EAL3 augmented with systematic flaw remediation (ALC_FLR.3). The report concludes that the product has met the target assurance level of EAL3 augmented with ALC_FLR.3 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 the AISEF evaluation facility Computer Science Corporation (CSC) and was completed on 18 November 2010.

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

a) used only in its evaluated configuration;

b) using IP filter rules to restrict the IP ranges which have access to the TOE.

c) operated according to the administrator's guidance, ensuring the TOE's administrator's password is changed from the default value immediately on setup. There is only one administrator's password and sharing this compromises administrator's accountability.

d) located in a secure area, visible to the workgroup using the MFD; and

e) cleared of pending print jobs and printed documents promptly.

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

6 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 Security Target (Ref [1]), and read this Certification Report prior to deciding whether to purchase the product.

Table of Contents

Chapter 1 - Introduction

1.1 Overview

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

1.2 Purpose

8 The purpose of this Certification Report is to:

a) report the certification of results of the IT security evaluation of the TOE, Xerox WorkCentre 4250 and 4260 Multifunction Systems against the requirements of the Common Criteria (CC) evaluation assurance level EAL3+; and

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

9 This report should be read in conjunction with the TOE's Security Target (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

10 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	Xerox WorkCentre 4250 and 4260 Multifunction Systems		
Software Version	Item	4250	4260
	System Software Main Controller IOT Software UI Network Controller Document Feeder Software Finisher Software (optional) Tray Firmware (optional)	15.003.32.000 2.50.03.32 0.01.17 0.045.15.027 4.01.23 1.01 4.04.09 1.01.04	30.103.32.000 2.50.03.32 0.40.59 0.040.15.176 4.01.67 1.01 4.04.09 1.01.04
Security Target	Xerox WorkCentre 4250 and 4260 Multifunction Systems Security Target version 1.0 (November 2010)		
Evaluation Assurance Level	EAL3 + ALC_FLR.3		

Evaluation Technical Report	WorkCentre 4250/4260 Evaluation Technical Report version 2.0, 18 NOV 2010
Criteria	Common Criteria for Information Technology Security Evaluation, Version 3.1, CCMB 2006-09-001 September 2006 Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; Version 3.1, Revision 2, CCMB-2007-09-002,
Methodology	Common Methodology for Information Technology Security Evaluation, Evaluation methodology, Version 3.1 Revision 2, CCMB-2007-09-003, September 2007
Conformance	CC Part 2 Conformant CC Part 3 Augmented with systematic flaw remediation (ALC_FLR.3).
Sponsor/ Developer	Xerox Corporation
Evaluation Facility	CSC Australia

Chapter 2 - Target of Evaluation

2.1 Overview

11 This chapter contains information about the Target of Evaluation (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

12 The TOE is the Xerox WorkCentre 4250 and 4260 Multifunction Systems developed by Xerox Corporation. Their primary role is to copy and print, with scan-to-e-mail, network scan and fax option.

13 The TOE provides an image overwrite package that operates two independent settings. One is the immediate image overwrite setting (IIO). This function forces any temporary image files created on the hard disk drive during a copy, print, network scan or scan-to-email to be overwritten when those files are no longer needed. Alternatively the overwrite process can be performed by an administrator “on demand” known as on-demand image overwrite (ODIO).

14 The TOE stores temporary image data created during a copy (landscape/stapled type only), print, network scan or scan to e-mail job on an internal hard disk drive (HDD). This temporary image data consists of the original data submitted and additional files created during a job. Because FAX jobs are not written to the HDD, there are no temporary images files to be overwritten for this service. Print, network scan and scan to e-mail jobs are written directly to the HDD when the job enters the system. Copy jobs are buffered in volatile memory with one exception: only copy jobs of type "landscape/stapled" are written to the disk. Any data that gets written to the disk will be overwritten at the completion of the job.

2.3 Security Policy

15 The TOE Security Policy (TSP) is a set of rules that defines how the information within the TOE is managed and protected. The TSP is defined in the Security Target (Ref [1]). A summary of the TSP is provided below:

i) User data protection policy;

ii) Information flow control policy;

iii) SSL security function policy;

i) IP filter security function policy; and

ii) Privileged user access security function policy.

2.4 TOE Architecture

16 The TOE consists of the following subsystems:

a) **Copy Controller subsystem**

The Copy Controller provides all of the functions necessary to implement a digital copier, and works together with the fax card to implement embedded fax functionality. The Copy Controller contains the image path, which uses proprietary hardware and algorithms to process the scanned images into high quality reproductions. Among other common copier functions, the Mass Storage Controller (MSC) works with the dynamic random access memory (DRAM) to enable electronic pre-collation, sometimes referred to as scan-once/print-many.

b) **Network Controller subsystem**

The Network Controller provides both network and direct-connect external interfaces, and enables print, email, network scan, and LanFAX functionality. The Network Controller also incorporates an open-source web server (Apache) that exports a Web User Interface (WebUI) through which users can submit jobs and check job and machine status, and

through which system administrators can remotely administer the machine.

c) **Fax card subsystem**

The embedded FAX service uses an optionally installed embedded fax card to send and receive images over the telephone interface. The FAX card plugs into a local bus on the copy controller.

d) **Scanner subsystem.**

The purpose of the Scanner Subsystem is to provide mechanical transport of hardcopy originals and to convert hardcopy originals to electronic data.

e) **Graphical User Interface (GUI) subsystem**

The GUI Subsystem detects soft and hard button actuations at the local user interface, and provides text and graphical prompts to the user. The GUI is sometimes referred to as the Local User Interface (LUI) to distinguish it from the WebUI which is exported by the web service that runs in the Network Controller.

f) **Marking Engine subsystem**

The Marking Engine performs copy or print paper feeding and transport, image marking and fusing, and document finishing. Images are not stored at any point in these subsystems.

2.5 Clarification of Scope

17 The scope of the evaluation was limited to those claims made in the Security Target (Ref [1]). It includes all software and firmware that are installed on the product.

2.5.1 Evaluated Functionality

18 The TOE evaluated security functionality is described in detail in the Security Target (Ref [1]) and includes:

a) image overwrite;

b) information flow;

c) system authentication;

d) network authentication;

e) security audit;

f) cryptographic support;

g) user data protection using SSL, IP filtering ,IPSEC and AES;

h) identification and authentication;

i) network management; and

j) security management;

2.5.2 Non-evaluated Functionality and Services

19 Potential users of the TOE are advised that some functions and services have not 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 Australian Government Information and Technology Security Manual (ISM) (Ref [2]) for policy relating to using an evaluated product in an un-evaluated configuration. New Zealand Government users should consult the Government Communications Security Bureau (GCSB).

2.6 Usage

2.6.1 Evaluated Configuration

20 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 the ISM (Ref [2]) to ensure that configuration(s) meet the minimum Australian Government policy requirements. New Zealand Government users should consult the Government Communications Security Bureau (GCSB).

21 The TOE is comprised of the software components identified in the Security Target (Ref [1]).

2.6.2 Delivery procedures

22 When placing an order for the TOE, purchasers should make it clear to their supplier that they wish to receive the evaluated product and version.

23 The following delivery procedures will be utilised during delivery of the TOE:

a) A customer representative at the delivery centre will contact the customer to arrange a delivery date.

b) A Xerox Authorised Representatives (XAR) or a local delivery contractor (e.g. UPS) will deliver the device to the customer site.

c) The XAR or the customer will install the TOE per installation instructions. If there is an issue during delivery, the XAR will order and install replacement parts, or commence re-delivery of the TOE if necessary.

2.6.3 Determining the Evaluated Configuration

24 In accordance with the Security Target delivery and installation of the TOE will be by a XAR using the appropriate Xerox delivery and installation guidance. This provides assurance that the correct version of the TOE has been delivered.

25 For additional assurance, it is recommended end users of the TOE verify the following:

a) **Model:** To verify that the correct model has been delivered, inspect the front of the device for a model number. WorkCentre 4250 or 4260 should be clearly labelled on the front of the unit. If this cannot be found, on the rear of the copier there should be a Xerox Corporation sticker that identifies the 'WorkCentre 4250' or '4260' model number along with the device serial number and other information.

b) **Features:** Ensure that all components received (including optional features) are consistent with those ordered. Confirm that the features received are consistent with the features identified for the model and ensure all required features as identified in the evaluated configuration are installed.

c) **Firmware:** After powering on the device, print a configuration page via the LUI. Verify the device firmware version is consistent with the version stated in Security Target (Ref [1]). If the firmware is not consistent with the Security Target, update the version as per the administrator guidance (Ref [3]).

2.6.4 Product Installation.

26 It is intended that the TOE will be installed by a XAR and configured by the system administrator. The System Administrator must ensure the TOE is configure in reference to the Preparative Procedures (ref [3]b) in order to ensure the TOE is in the evaluated configuration. Key points that must be followed from the procedures include:

a) Changing the Administrative password, ensuring the TOE's administrator's password is changed from the default value immediately on setup. There is only one administrators password and sharing this compromises administrator's accountability;

b) Configuring security features. The TOE provides the ability for the system administrator to configure a network information flow control policy based on a configurable rule set. The information flow control policy is generated by the system administrator specifying a series of rules to "accept" packets. These rules include a listing of IP addresses that will be allowed to communicate with the TOE;

c) Installing Optional components;

d) Disabling cloning and Software upgrades; and

e) Enabling the admin pin security feature for the diagnostics menu.

2.6.5 Documentation

27 It is important that the TOE is used in accordance with guidance documentation in order to ensure secure usage. The following documentation is provided with the TOE:

i) User Guidance CD-ROM, ID: 538N00084 rev A. The User Guidance CD-ROM contains a PDF document that provides in-depth configuration and usage instructions for the TOE. The guidance serves to assist both the administrator and users of the TOE.

ii) Administrative Guidance CD-ROM, ID: 538N00088 rev A. The Administrative Guidance CD-ROM contains an interactive flash program that serves to assist the administrator in configuring all features of the TOE.

iii) Installation Instructions, The following documentation is available via the Xerox website: (http://www.xerox.com/information-security/product/enus.html) 'Secure Installation and Operation of your WorkCentre 4250/4260, March 22 , 2010, version 1.1.'

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

29 Section 3: 'TOE Security Environment' in the Security Target (Ref [1]) provides a full description of the assumptions. Assumptions are made in the following areas:

a) installation;

b) access;

c) management;

d) administration;

e) network;

f) control;

g) compliance;

h) pins (System administrators eight character pin is changed every 40 days and a nine character pin is changed every year); and

i) procedures.

Chapter 3 - Evaluation

3.1 Overview

30 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

31 The criteria against which the Target of Evaluation (TOE) has been evaluated are contained in the Common Criteria for Information Technology Security Evaluation (Refs [4], [5] and [6]). The methodology used is described in the Common Methodology for Information Technology Security Evaluation (CEM) (Ref [7]). The evaluation was also carried out in accordance with the operational procedures of the Australasian Information Security Evaluation Program (AISEP) (Refs [8], [9], [10] and [11]). In addition, the conditions outlined in the Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security (Ref [12]) were also upheld.

3.3 Functional Testing

32 To gain confidence that the developer's testing was sufficient to ensure the correct operation of the TOE, the evaluators analysed the evidence of the developer's testing effort. This analysis included examining: test coverage; test plans and procedures; and expected and actual results. The evaluators drew upon this evidence to perform a sample of the developer tests in order to verify that the test results were consistent with those recorded by the developers. The security features tested by the evaluators were:

a) cryptographic algorithms;

b) audit;

c) admin pin strength;

d) image overwrite;

e) system authentication;

f) network authentication;

g) SSL and audit logs;

h) TOE administration;

i) IP filtering; and

j) diagnostics functionality and SNMP

3.4 Penetration Testing

33 The developer performed a vulnerability analysis of the TOE in order to identify any obvious vulnerability in the product and to show that the vulnerabilities were not exploitable in the intended environment of the TOE. This analysis included a search for possible vulnerability sources in publicly available information.

Chapter 4 - Certification

4.1 Overview

34 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

35 After due consideration of the conduct of the evaluation as witnessed by the certifiers, and of the Evaluation Technical Report (Ref [13]), the Australasian Certification Authority certifies the evaluation of Xerox WorkCentre 4250 and 4260 Multifunction Systems performed by the Australasian Information Security Evaluation Facility, CSC.

36 CSC has found that Xerox WorkCentre 4250 and 4260 Multifunction Systems upholds the claims made in the Security Target (Ref [1]) and has met the requirements of Common Criteria (CC) evaluation assurance level EAL3 augmented with systematic flaw remediation (ALC_FLR.3)

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

38 EAL3 provides assurance by an analysis of the security functions, using a functional and interface specification, guidance documentation, and the high-level design of the TOE, to understand the security behaviour.

39 The analysis is supported by independent testing of the TOE security functions, evidence of developer testing based on the functional specification and high-level design, selective independent confirmation of the developer test results, strength of function analysis, and evidence of a developer search for obvious vulnerabilities (e.g. those in the public domain).

40 EAL3 also provides assurance though the use of development environment controls, TOE configuration management, and evidence of secure delivery procedures.

4.3 Recommendations

41 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 the ISM (Ref [2]) and New Zealand Government users should consult the Government Communications Security Bureau (GCSB).

42 In addition to ensuring that the assumptions concerning the operational environment are fulfilled and the guidance document is followed (Ref [3]), the ACA also recommends that users and administrators ensure that the TOE is:

a) used only in its evaluated configuration;

b) using IP filter rules to restrict the IP ranges which have access to the TOE.

c) operated according to the administrator's guidance, ensuring the TOE's administrator's password is changed from the default value immediately on setup. There is only one administrators password and sharing this compromises administrator's accountability.

d) located in a secure area, visible to the group using the MFD; and

e) cleared of pending print jobs and documents promptly.

Annex A - References and Abbreviations

A.1 References

[1] Xerox WorkCentre 4250/4260 Multifunction Systems Security Target version 1.0, (November 2010).

[2] Australian Government Information and Communications Technology Security Manual (ISM), 2009, Defence Signals Directorate, (available at www.dsd.gov.au).

[3] Product Documentation:

a) User Guidance CD ROM ID: 538N00084 rev A

b) Administration Guidance CD ROM ID: 538N00088 rev A.

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

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

[6] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components September 2007 Version 3.1 Revision 2 CCMB-2009-07-003.

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

[8] AISEP Publication No. 1 – Program Policy, AP 1, Version 3.1, 29 September 2006, Defence Signals Directorate.

[9] AISEP Publication No. 2 – Certifier Guidance, AP 2. Version 3.1,29 September 2006, Defence Signals Directorate.

[10] AISEP Publication No. 3 – Evaluator Guidance, AP 3. Version 3.1, 29 September 2006, Defence Signals Directorate

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

[12] Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, May 2000

[13] WorkCentre 4250/4260 Evaluation Technical Report version 2.0, 18 November 2010.

A.2 Abbreviations

AISEF	Australasian Information Security Evaluation Facility
AISEP	Australasian Information Security Evaluation Program
CC	Common Criteria
CEM	Common Evaluation Methodology
DSD	Defence Signals Directorate
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GCSB	Government Communications Security Bureau
IIO	Immediate Image Overwrite
LUI	Local user interface
ODIO	On-demand image overwrite
PP	Protection Profile
SFP	Security Function Policy
SFR	Security Functional Requirements
SSL	Secure Sockets Layer
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy
XAR	Xerox Authorised Representative
+	augmented