THE DOCUMENT COMPANY

XEROX®

Xerox CopyCentre C65/C75/C90 Copier
and
WorkCentre Pro 65/75/90 Advanced Multifunction System including Image Overwrite Security Security Target

Version 1.0

Prepared by:

Xerox Corporation
250 Cross Keys Office Park
Fairport, New York 14450

Computer Sciences Corporation
132 National Business Parkway
Annapolis Junction, MD 20701

Date	Revision	Changes Made
April 30, 2003	1.0	Original Draft
May 5, 2004	1.1	First draft to CVS
May 5, 2004	1.2	Second attempt at CVS
May 6, 2004	1.3	Changes in response to XRM_EDR_001 and general editing changes for clarity
May 11, 2004	1.4	Document resized via figure changes
May 12, 2004	1.5	Changes in response to XRM_EDR_002/003/004
May 19, 2004	1.6	Changes in response to XRM_EDR_005/006
May 20, 2004	1.7	Changes in response to XRM_EDR_007 and additional clarifications
June 3, 2004	1.8	Changes in response to XRM_EDR_010 and addition of assumption addressing removable hard drive issue
June 17, 2004	1.9	Changes in response to XRM_EDR_012
July 1, 2004	1.10	Changes in response to XRM_EDR_014/016 and further clarification of the removable hard drive issue
July 7, 2004	1.11	Correction of typographical/grammatical errors and clarification of minor points
September 13, 2004	1.12	Changes in response to XRM_EDR_022, correction of typographical/grammatical errors, and clarification of minor points
December 17, 2004	1.13	Changed Network Controller software version number to reflect latest patches.
January 5, 2005	1.14	Changed “with” to “including” in the TOE title and all other TOE references.

Table of Contents

List of Figures

List of Tables

1 SECURITY TARGET INTRODUCTION

1 This Chapter presents security target (ST) identification information and an overview of the ST. An ST contains the information technology (IT) security requirements of an identified Target of Evaluation (TOE) and specifies the functional and assurance security measures offered by that TOE to meet stated requirements. An ST principally defines:

a) A security problem expressed as a set of assumptions about the security aspects of the environment, a list of threats that the product is intended to counter, and any known rules with which the product must comply (Chapter 3, TOE Security Environment).

b) A set of security objectives and a set of security requirements to address the security problem (Chapters 4 and 5, Security Objectives and IT Security Requirements, respectively).

c) The IT security functions provided by the TOE that meet the set of requirements (Chapter 6, TOE Summary Specification).

2 The structure and content of this ST comply with the requirements specified in the Common Criteria (CC), Part 1, Annex C, and Part 3, Chapter 5.

1.1 ST and TOE Identification

3 This section provides information needed to identify and control this ST and its Target of Evaluation (TOE). This ST targets Evaluation Assurance Level (EAL)2.

ST Title:	Xerox CopyCentre C65/C75/C90 Copier and WorkCentre Pro 65/75/90 Advanced Multifunction System including Image Overwrite Security Security Target
ST Version:	1.0
Revision Number:	$Revision: 1.12 $
Publication Date:	$Date: 2004/09/13 12:51:06 $
Authors:	Computer Sciences Corporation, Common Criteria Testing Laboratory
TOE Identification:	Xerox CopyCentre C65/C75/C90 Copier and WorkCentre Pro 65/75/90 Advanced Multifunction System including Image Overwrite Security.
CC Identification:	Common Criteria for Information Technology Security Evaluation, Version 2.1, August 1999 (also known as ISO 15408)
ST Evaluator:	Computer Sciences Corporation (CSC)
Keywords:	Xerox, Multi Function Device, Image Overwrite

1.2 References

4 The following documentation was used to prepare this ST:

[CC_PART1]	Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated August 1999, version 2.1, CCIMB-99-031, Incorporated with interpretations as of 2003-12-31
[CC_PART2]	Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated August 1999, version 2.1, CCIMB-99-032, Incorporated with interpretations as of 2003-12-31.
[CC_PART3]	Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated August 1999, version 2.1, CCIMB-99-033, Incorporated with interpretations as of 2003-12-31.
[CEM_PART1]	Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and General Model, dated 1 November 1997, version 0.6.
[CEM_PART2]	Common Methodology for Information Technology Security Evaluation – Part 2: Evaluation Methodology, dated August 1999, version 1.0, Incorporated with interpretations as of 2003-12-31.

1.3 Conventions, Terminology, and Acronyms

5 This section identifies the formatting conventions used to convey additional information and terminology. It also defines terminology and the meanings of acronyms used throughout this ST.

1.3.1 Conventions

6 This section describes the conventions used to denote Common Criteria (CC) operations on security functional components and to distinguish text with special meaning. The notation, formatting, and conventions used in this ST are largely consistent with those used in the CC. Selected presentation choices are discussed here.

7 The CC allows several operations to be performed on security functional components; *assignment, refinement*, *selection,* and *iteration* as defined in paragraph 2.1.4 of Part 2 of the CC are:

a) The *assignment* operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Showing the value in square brackets [assignment_value(s)] indicates an assignment.

b) The *refinement* operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold text**.

c) The *selection* operation is used to select one or more options provided by the CC in stating a requirement. Selections are denoted by *underlined italicized text.*

d) *Iterated* functional components are given unique identifiers by appending to the component name, short name, and functional element name from the CC an iteration number inside parenthesis, i.e., FMT_MTD.1.1 (1) and FMT_MTD.1.1 (2).

e) Plain *italicized text* is used to emphasize text.

1.3.2 Terminology

8 In the CC, many terms are defined in Section 2.3 of Part 1. The following terms are a subset of those definitions:

Authentication data	Information used to verify the claimed identity of a user.
External IT entity	Any IT product or system, untrusted or trusted, outside of the TOE that interacts with the TOE.
Object	An entity within the TOE Security Function (TSF[1]) Scope of Control (TSC[2]) that contains or receives information and upon which subjects perform operations.
Role	A predefined set of rules establishing the allowed interactions between a user and the TOE.
Security Functional Components	Express security requirements intended to counter threats in the assumed operating environment of the TOE.
Subject	An entity within the TSC that causes operations to be performed.

9 The following terminology is specific to this ST:

Image Data	Information on a mass storage device created by the copy/print/scan/email/fax processes.
Latent Image Data	Residual information remaining on a mass storage device when a copy/print/scan/email/fax job is completed or cancelled.
Non-privileged User	For the purposes of this evaluation, the term “non-privileged user” applies to all individuals who operate or use TOE features without any administrative rights or privileges.
System Administrator	A user who manages the Xerox Corporation CopyCentre C65/C75/C90 or WorkCentre Pro 65/75/90.
User	For the purposes of this evaluation, the term “user” applies only to TOE system administrators, except in generalized usage, such as “local user interface” or Web user interface.”.

1.3.3 Acronyms

10 The following acronyms are used in this Security Target:

As defined in the CC, Part 1, version 2.1:
1 TSF - A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.
2 TSC - The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.

ACRONYM	DEFINITION
AUT	Authentication
CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Evaluation Methodology for Information Technology Security
CM	Configuration Management
DC	Digital Copier
EAL	Evaluation Assurance Level
FDP	User Data Protection CC Class
FIA	Identification and Authentication CC Class
FMT	Security Management CC Class
FPT	Protection of Security Functions
FSP	Functional Specification
HDD	Hard Disk Drive
HLD	High Level Design
ISO	International Standards Organization
ISO 15408	Common Criteria 2.1 ISO Standard
IT	Information Technology
MFD	Multifunction Device
MOF	Management of Functions
MTD	Management of TSF Data
OSP	Organization Security Policy
PP	Protection Profile
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SM	Security Management
SMR	Security Management Roles
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy
UAU	User Authentication
UDP	User Data Protection

1.4 TOE Overview

11 Two configurations of the TOE with identical security functionality are under evaluation. The base configuration is a digital copier device (copy only). The other configuration adds several options (print, scan-to-email, network scan, and network fax) to the base configuration to yield a multi-function device (MFD). The evaluated configuration of both the copier and MFD includes the Image Overwrite Security package, a consumer option. This package causes any temporary

image files created during a copy, print, network scan, scan-to-email, or network fax job to be overwritten when those files are no longer needed or "on demand" by the system administrator.

12 An additional consumer option on both configurations offers external removable hard disk drive(s) mounted in a separate cabinet and connected to the TOE by a SCSI cable. This option is intended for high-security environments, including those that require that disk drives be physically removed and stored in a GSA-approved security container in order to conform to National Industrial Security Program (NISP) security requirements. Each drive bay in the external cabinet is secured by a barrel lock. This option is also included within the evaluation boundary of both the multi-function device and the digital copier device.

13 A summary of the TOE security functions can be found in Section 2, TOE Description. A detailed description of the security functions can be found in Section 6, TOE Summary Specification.

1.5 Common Criteria Conformance Claim

14 This ST conforms to CC Part 2 conformant and is CC Part 3 conformant at the EAL 2 level of assurance.

2 TOE DESCRIPTION

15 This section provides context for the TOE evaluation by identifying the product type and describing the evaluated configuration.

2.1 Product Type

16 There are two configurations of the TOE with identical security functionality under evaluation. The base configuration is as a digital copier that provides only copy functions (hereafter referred to as a DC), represented by the CopyCentre models. The other configuration is as a multi-function device that copies, prints, scans to e-mails, network scans, and network faxes (hereafter referred to as a MFD), represented by the WorkCentre Pro models. The MFD models contain two internal hard disk drives (referred to as Network Controller HDD and Copy Controller HDD respectively); DC models contain only one internal drive (referred to as the Copy Controller HDD). The evaluated configuration of both the DC and MFD includes the Image Overwrite Security package, a consumer option. The Image Overwrite Security package causes any temporary image files created during a print, network scan, scan-to-email, network fax (MFD), or copy (MFD/DC) job to be erased from the internal hard disk drive(s) when those files are no longer needed or on demand at the discretion of the system administrator.

17 An additional consumer option offered on both the DC and MFD models is a provision for external removable hard disk drive(s) mounted in a separate cabinet and connected to the TOE by a SCSI cable. The internal hard disk drive(s) must be removed to allow connection of the external cabinet. Each drive bay in the external cabinet is secured by a barrel lock when the TOE is in use. This option is intended for high-security environments where hard disk drives must be securely stored outside of normal operating hours. This option is also included within the evaluation boundary of both the multi-function device and the digital copier device.

Table 1: Models and Capabilities

	Print	Copy	Network Scan	Scan-to-email	Network Fax
CopyCentre C65	n/a	x	n/a	n/a	n/a
CopyCentre C75	n/a	x	n/a	n/a	n/a
CopyCentre C90	n/a	x	n/a	n/a	n/a
WorkCentre Pro 65	x	x	o	o	o
WorkCentre Pro 75	x	x	o	o	o
WorkCentre Pro 90	x	x	o	o	o

18 On MFD models, copy jobs are submitted via the Local UI directly to the Copy Controller. Print jobs submitted via the Web UI are passed by the Network Controller to the Copy Controller. Once processed by the Copy Controller, copy and print jobs are sent to the Image Output Terminal. Network scan, scan-to-email, and network fax jobs are submitted via the Local UI to the Copy Controller which, upon recognition that the job is neither a copy nor print job, passes the job to the Network Controller for processing. Each time a job transits or is processed by one of the controllers, temporary image data, consisting of the original data submitted and any additional files created during job processing, is created and stored on the controller HDDs.

19 On DC models, copy jobs are submitted via the Local UI to the Copy Controller and, after processing, are sent to the Image Output Terminal. Temporary image data, consisting of the original data submitted and any additional files created during the processing of each copy job, is created and stored on the Copy Controller HDD.

20 The TOE provides image overwrite functions (TSF_IOWN and TSF_IOWC for the MFD and TSF_IOWC for the DC) to enhance the security of both models. The image overwrite function overwrites temporary document image data as described in DoD Standard 5200.28-M at the completion of each print, network scan, scan-to-email, network fax (MFD), and copy (MFD/DC) job or *on demand* of the system administrator. A system administrator may use the "on demand" image overwrite security function to clear sensitive information from the Network and Copy Controller HDDs when the MFD is decommissioned, for example. TSF_IOWN overwrites data stored on the Network Controller HDD (MFD) and TSF_IOWC overwrites data stored on the Copy Controller HDD (MFD and DC).

2.1.1 Physical Scope and Boundary

21 The physical appearance of the DC (CopyCentre C65/C75/C90) and MFD (WorkCentre Pro 65/75/90) models is identical and is depicted in Figure 1.

Figure 1: Xerox CopyCentre/WorkCentre Pro

22 The figure shows an optional paper feeder and finisher. The external removable HDD cabinet is not shown.

Table 2: Evaluated Software/Firmware version

Software/Firmware Item	CopyCentre C65/C75/C90	WorkCentre Pro 65/75/90

System Software	1.001.02.074	1.001.02.074
Network Controller Software	Not Included	1.02.074.02.P17.P18
UI Software	001.02.068	001.02.068
IOT Software (Copy Controller Software)	01.02.74	01.02.74
Finisher Software	16.20	16.20

2.1.2 Logical Scope and Boundary

23 The TOE logical boundary for both the MFD and DC have the following security functions controlled by the TOE:

- Image Overwrite Network Controller (TSF_IOWN) (MFD only)
- Image Overwrite Copy Controller (TSF_IOWC)
- Authentication (TSF_AUT)
- Security Management (TSF_FMT)

24 During normal operation, the MFD or DC spools temporary document image data to the internal disks or disk. As illustrated in Figure 2, the image overwrite functions (TSF_IOWN and TSF_IOWC) clear temporary document image data from the internal or removable external disk(s) by writing over the image data with three specific patterns of data. The image overwrite functions clear data once a job is completed (Immediate Image Overwrite (IIO)) or when invoked at any time by the system administrator (On-Demand Image Overwrite (ODIO)).

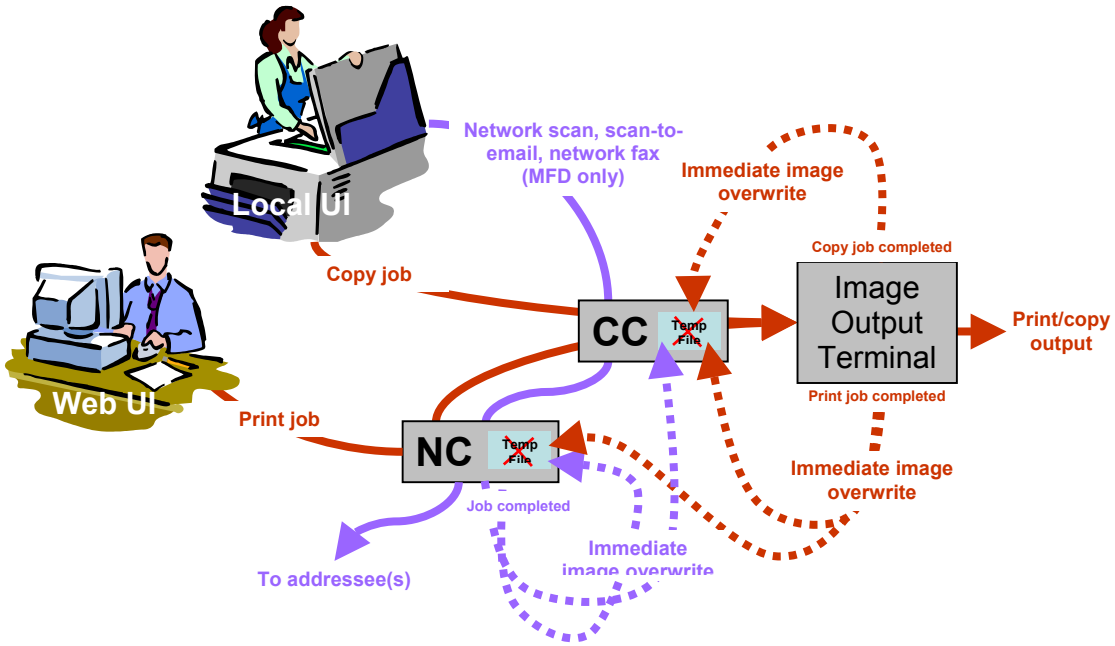

Figure 2. Immediate Image Overwrite

25 TSF_IOWN overwrites data stored on the Network Controller HDD (MFD) and TSF_IOWC overwrites data stored on the Copy Controller HDD (MFD and DC).

26 Only the system administrator, who is authenticated via a personal identification number (PIN) (TSF_AUT), can access the security settings of the MFD or DC (TSF_FMT). Non-privileged

users can utilize the other non-security-related features/functions of the MFD or DC without authentication.

3 TOE SECURITY ENVIRONMENT

3.1 Secure Usage Assumptions

27 This section describes the security aspects of the intended environment for the evaluated TOE. This includes information about the physical, personnel, procedural, connectivity, and functional aspects of the environment.

28 The operational environment must be managed in accordance with assurance requirement documentation for delivery, operation, and user/system administrator guidance. The following specific conditions are assumed to exist in an environment where this TOE is employed.

3.1.1 Environment Assumptions

29 The environmental assumptions delineated in Table 3 are required to ensure the security of the TOE:

Table 3: Environmental Assumptions

Assumption	Description
A.INSTALL	The TOE has been delivered, installed, and setup in accordance with documented delivery and installation/setup procedures.
A.MANAGE	There will be one or more competent system administrator(s) assigned to manage the TOE and the security of the information it contains.
A.NO_EVIL_ADM	The system administrator(s) are not careless, willfully negligent, nor hostile, and will follow and abide by the instructions provided by the system administration documentation.
A.PROCEDURE	Procedures exist for granting system administrator(s) access to the TSF.
A.CHANGE_KOC	System administrators PIN is changed according to the following: 8-digit PIN every 40 days 9-digit PIN every year
A.PHYSICAL_ PROTECT	The TOE will be located within facilities providing controlled (i.e., employee-only) access to prevent unauthorized physical access to internal parts of the TOE, the TOE serial port, and/or the external HDD cabinet (if present).

3.2 Threats

30 Table 4 identifies the threats to the TOE. The threats to the TOE are considered to be non-privileged users with public knowledge of how the TOE operates. While the threat may have limited routine access to the TOE, it is not likely that the threat would have the prolonged

physical access necessary to remove TOE internal HDD(s) or to connect to the TOE via the serial port to copy latent image data. Similarly, the threat would not have time to forcibly remove the drive(s) from the removable HDD cabinet or to disconnect the cabinet and remove it from the facility without being challenged. Further, the threat is not judged to have the sophistication or resources necessary to recover latent image data from a HDD. Mitigation of the threats is through the objectives identified in Section 4, Security Objectives.

Table 4: Threats to the TOE

Threat	Description
T.RECOVER	A malicious, non-privileged user may attempt to recover temporary document image data from a copy/print/network scan/scan-to-email/network fax job by removing the internal disks or disk and using commercially available tools to read its contents. This scenario may occur as part of the life-cycle of the MFD/DC (e.g., decommission) or as a more overt action that could include attempts to remove the external HDD cabinet (if present) from the facility.

3.3 Organizational Security Policies

31 There are no organizational security policies that are determined to be relevant for the TOE.

4 SECURITY OBJECTIVES

32 The purpose of the security objectives is to detail the response planned to counter to a security problem or identified threat. Threats can be directed against the TOE or the security environment or both, therefore, the CC identifies two categories of security objectives:

- Security objectives for the TOE, and
- Security objectives for the environment.

4.1 Security Objectives for the TOE

33 This section identifies and describes the security objectives of the TOE.

34 The TOE accomplishes the security objectives defined in Table 5.

Table 5: Security Objectives for the TOE

Objectives	Description
O.RESIDUAL	Temporary document image data from a job must not remain on the hard disk drive(s) once that job is completed.
O.MANAGE	Only System Administrators shall have the capability to exercise security management functions provided by the TSF.
O.ONDEMAND	The TOE will provide the system administrator with the ability to invoke the image overwrite function “on demand.”

4.2 Security Objectives for the Non-IT Environment

35 The security objectives for the IT Environment are defined in Table 6.

Table 6: Security Objectives for the Non-IT Environment

Objectives	Description
OE.MANAGE	A responsible individual will be assigned as the system administrator who will see that the TOE is installed, and is operated in accordance with all applicable policies and procedures necessary to operate the TOE in a secure manner.
OE.PHYSICAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are effectively protected against physical attack within the facility. In high-security environments where the removable hard drive (RHD) option has been selected, that protection must include measures to prevent the removal of the RHD cabinet from the facility.

5 IT SECURITY REQUIREMENTS

36 This section defines the IT security requirements that shall be satisfied by the TOE or its environment:

37 The CC divides TOE security requirements into two categories:

- Security functional requirements (SFRs) (such as, identification and authentication, security management, and user data protection) that the TOE and the supporting evidence need to satisfy to meet the security objectives of the TOE.
- Security assurance requirements (SARs) that provide grounds for confidence that the TOE and its supporting IT environment meet its security objectives (e.g., configuration management, testing, and vulnerability assessment).

38 These requirements are discussed separately within the following subsections.

5.1 TOE Security Functional Requirements

39 The TOE satisfies the SFRs delineated in Table 7. The rest of this section contains a description of each component and any related dependencies.

Table 7: TOE Security Functional Requirements

Functional Component ID	Functional Component Name
FDP_RIP.1 (1)	Subset Residual Information Protection
FDP_RIP.1 (2)	Subset Residual Information Protection
FIA_UID.2	User Identification before any Action
FIA_UAU.2	User Authentication before any Action
FIA_UAU.7	Protected Authentication Feedback
FMT_MOF.1	Management of Security Functions Behavior
FMT_SMF.1	Specification of management functions
FMT_SMR.1	Security Roles

5.1.1 Class FDP: User Data Protection

40 FDP_RIP.1 (1) Subset Residual Information Protection

Hierarchical to: No other components

FDP_RIP.1.1(1) The TSF shall ensure that any previous information content of a resource is made unavailable upon the *deallocation of the resource from* the following objects: [

Network Controller Hard Disk Drive

Dependencies: No dependencies

41 FDP_RIP.1 (2) Subset Residual Information Protection

Hierarchical to: No other components

FDP_RIP.1.1(2) The TSF shall ensure that any previous information content of a resource is made unavailable upon the *deallocation of the resource from* the following objects: [

Copy Controller Hard Disk Drive

Dependencies: No dependencies

5.1.2 Class FIA: Identification and Authentication

42 FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1

FIA_UID.2.1 The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: No dependencies

43 FIA_UAU.2 User Authentication Before Any Action

Hierarchical to: FIA_UAU.1 Timing of Authentication

FIA_UAU.2.1 The TSF shall require each **system administrator** to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that **system administrator**.

Dependencies: FIA_UID.1 Timing of Identification

44 FIA_UAU.7 Protected Authentication Feedback

Hierarchical to: No other components

FIA_UAU.7.1 The TSF shall provide only [obscured feedback] to the **system administrator** while the authentication is in progress.

Dependencies: FIA_UAU.1 Timing of Authentication

5.1.3 Class FMT: Security Management

45 FMT_MOF.1 Management of Security Functions Behavior

Hierarchical to: No other components

FMT_MOF.1.1 The TSF shall restrict the ability to *disable* and *enable* the functions [TSF_IOWN, TSF_IOWC] to [the system administrator].

Dependencies: FMT_SMR.1 Security Roles
FMT_SMF.1 Specification of management functions

46 FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: [

Enable/disable Immediate Image Overwrite (IIO) [TSF_IOWN, TSF_IOWC],

Change PIN,
Invoke/Abort ODIO [TSF_IOWN, TSF_IOWC]

Dependencies: No Dependencies

47 FMT_SMR.1 Security roles

Hierarchical to: No other components.

FMT_SMR.1.1 The TSF shall maintain the roles [system administrator].

FMT_SMR.1.2 The TSF shall be able to associate **human** users with roles.

Dependencies: FIA_UID.1 Timing of identification

5.2 TOE Security Assurance Requirements

48 Table 8 identifies the security assurance components drawn from CC Part 3 Security Assurance Requirements EAL2. The SARs are not iterated or refined from Part 3.

Table 8: EAL2 Assurance Requirements

Assurance Component ID	Assurance Component Name	Dependencies
ACM_CAP.2	Configuration items	None
ADO_DEL.1	Delivery procedures	None
ADO_IGS.1	Installation, generation, and start-up procedures	AGD_ADM.1

Assurance Component ID	Assurance Component Name	Dependencies
ADV_FSP.1	Informal functional specification	ADV_RCR.1
ADV_HLD.1	Descriptive high-level design	ADV_FSP.1, ADV_RCR.1
ADV_RCR.1	Informal correspondence demonstration	None
AGD_ADM.1	Administrator guidance	ADV_FSP.1
AGD_USR.1	User guidance	ADV_FSP.1
ATE_COV.1	Evidence of coverage	ADV_FSP.1, ATE_FUN.1
ATE_FUN.1	Functional testing	None
ATE_IND.2	Independent testing-sample	ADV_FSP.1, AGD_ADM.1, AGD_USR.1, ATE_FUN.1
AVA_SOF.1	Strength of TOE security function evaluation	ADV_FSP.1, ADV_HLD.1
AVA_VLA.1	Developer vulnerability analysis	ADV_FSP.1, ADV_HLD.1 AGD_ADM.1, AGD_USR.1

5.3 Security Requirements for the IT Environment

49 There are no security functional requirements for the IT Environment.

5.4 Explicitly Stated Requirements for the TOE

50 There are no explicitly stated requirements for the TOE.

5.5 SFRs With SOF Declarations

51 The overall Strength of Function (SOF) claim for the TOE is SOF-basic.

52 FIA_UAU.2: The authentication mechanism has a PIN space of 10^3 – 10^{12} (3 – 12 digit PIN). Through Xerox guidance, the recommend PIN size is 8 to 12 digits (PIN Space of 10^8 to 10^{12}). System administrator PINs are changed every 40 days (8-digit PIN) or annually (9-digit PIN).

6 TOE SUMMARY SPECIFICATION

53 This section presents an overview of the security functions implemented by the TOE and the Assurance Measures applied to ensure their correct implementation.

6.1 TOE Security Functions

54 This section presents the security functions performed by the TOE to satisfy the identified SFRs in Section 5.1.1. Traceability to SFRs is also provided.

6.1.1 Image Overwrite Network Controller (TSF_IOWN)

55 The MFD configuration of the TOE implements an image overwrite security function to overwrite temporary files created during the printing, network scan, scan to email, or network fax processes. (Image overwrite of the files created during copy jobs on the MFD is discussed in Section 6.1.2 following.) In the MFD, temporary files are created as a result of print, network scan, scan-to-email, or network fax processing on a reserved section (/tmp/spool or /tmp/scan_spool) of the Network Controller hard disk drive (HDD). The files are overwritten on the Network Controller HDD using a three pass overwrite procedure as described in DOD 5800.28-M upon job completion using the Immediate Image Overwrite (IIO) function or upon action by the system administrator using the "On-Demand" Image Overwrite (ODIO) function. The ODIO function can be manually invoked by the system administrator at any time (e.g., in situations where the IIO function fails).

56 In the MFD, ODIO is invoked by the System Administrator via the tools menu/web interface. Once invoked, the ODIO cancels all print, network scan, scan-to-email, or network fax jobs, halts the printer interface (MFD), and overwrites the contents of the sections for temporary image files on the Network Controller HDD. The entire machine then reboots. If the System Administrator attempts to activate diagnostics mode while ODIO is in progress, the request will be queued until the ODIO completes and then the system will enter diagnostic mode.

57 While ODIO is running, both the Local and Web User Interfaces display a message stating that ODIO is in progress and an abort button. If the System Administrator aborts ODIO, the process stops at a sector boundary. As part of the cancellation, the file system is rebuilt (e.g., the directory is clear, the I-nodes are initialized, and the system then reboots). During every reboot the system goes through a file system check that verifies the integrity of the directory, and the disks are remounted.

58 In the MFD, if either the Network Controller or Copy Controller crashes for any reason, the controller that crashed will make three attempts to reboot itself, with the still operating controller "watching." After three unsuccessful reboot attempts, the operating controller will schedule a reboot of the entire machine. During reboot, an Immediate Image Overwrite is automatically performed on the Network Controller as part of job recovery. There is no automatic overwrite of the Copy Controller, however. The system administrator must manually run ODIO to overwrite the sections for temporary image files on the Copy Controller HDD. In the MFD, the progress of all jobs is tracked in logs on the Network Controller HDD (for print, scan-to-email, network fax,

and network scan jobs) and the Copy Controller HDD (for copy jobs). During the reboot process, logs are tracked. Abnormally terminated jobs on the Network Controller HDD are automatically overwritten by the IIO function, while the system administrator must invoke ODIO to overwrite abnormally terminated jobs on the Copy Controller HDD.

59 **Functional Requirements Satisfied:** FDP_RIP.1(1)

6.1.2 Image Overwrite Copy Controller (TSF_IOWC)

60 Both the MFD and DC models of the TOE implement an image overwrite security function to overwrite the temporary files created on the Copy Controller HDD for copy jobs (MFD and DC), print jobs (MFD), and those created on the Copy Controller HDD during the "pass-through" of network scan, scan-to-email, and network fax jobs (MFD) to the Network Controller. On both models, the files are overwritten on the Copy Controller HDD using a three pass overwrite procedure as described in DOD 5800.28-M upon job completion using the Immediate Image Overwrite (IIO) function or upon action by the system administrator using the "On-Demand" Image Overwrite (ODIO) function. The ODIO function can be manually invoked by the system administrator at any time (e.g., in situations where the IIO function fails).

61 ODIO is invoked by the System Administrator via the tools menu on the DC and via either the tools menu or web interface on the MFD. Once invoked, ODIO cancels all pending jobs and overwrites the contents of the sections for temporary image files on the Copy Controller HDD. The entire machine then reboots. If the System Administrator attempts to activate diagnostics mode while ODIO is in progress, the request will be queued until the ODIO completes and then the system will enter diagnostic mode.

62 While ODIO is running, the Local User Interface will display a message stating that ODIO is in progress and an abort button. If the System Administrator aborts ODIO, the process stops at a sector boundary. As part of the cancellation, the file system is rebuilt (e.g., the directory is clear, the I-nodes are initialized, and the system then reboots). During every reboot the system goes through a file system check that verifies the integrity of the directory, and the disks are remounted.

63 In the DC, if the Copy Controller crashes, the system will automatically reboot itself. Again, there is no automatic overwrite of the sections for temporary image files on Copy Controller HDD in the DC configuration. The system administrator must manually run ODIO to overwrite the sections for temporary image files on Copy Controller HDD. In both the DC and MFD configurations, the progress of all jobs is tracked in a log on the Copy Controller HDD. During the re-boot process, the log is consulted for any abnormally terminated jobs. If there are abnormally terminated jobs in the log, the System Administrator is prompted to run ODIO via a message on the Local User Interface.

64 **Functional Requirements Satisfied:** FDP_RIP.1(2)

6.1.3 Authentication (TSF_AUT)

65 The TOE utilizes a simple authentication function through the front panel (DC and MFD) or web interface (MFD only). The system administrator must authenticate by entering a 3 to 12 digit PIN prior to being granted access to the *tools menu* and system administration functions. The system administrator must change the default PIN after installation is complete. System administrator PINs are changed every 40 days (8-digit PIN) or annually (9-digit PIN). While the system administrator is entering the PIN number, the TOE displays a '*' character for each digit entered to hide the value entered. The authentication mechanism has a PIN space of 10^3 to 10^{12}.

66 The Web user interface also requires the system administrator to enter a PIN and enter "admin" into the username field. The username prompt provided by the web server is not used but is provided for historical reasons. The only valid string is "admin," which is hard coded into the web server and cannot be changed. Additional system administrators cannot be added. The TOE does not associate user attributes or privileges based on username.

67 **Functional Requirements Satisfied:** FMT_SMR.1, FIA_UAU.2, FIA_UAU.7, FIA_UID.2

6.1.4 Security Management (TSF_FMT)

68 The TSF_FMT utilizes the front panel software module security mechanisms to allow only authenticated system administrators the capability to invoke or abort the ODIO function, enable or disable the IIO function, and change the system administrator PIN.

69 Additionally, TSF_FMT utilizes the web server authentication mechanism to allow only authenticated system administrators the capability to manually invoke or abort "On Demand" Image Overwrite (ODIO) through the web interface.

70 The TOE restricts access to the configuration of administrative functions to the system administrator.

71 **Functional Requirements Satisfied:** FMT_SMR.1, FMT_MOF.1, FMT_SMF.1

6.2 Assurance Measures

72 The TOE satisfies CC EAL2 assurance requirements. This section identifies the Configuration Management, Delivery and Operation, Development, Guidance Documents, Testing, and Vulnerability Assessment Assurance Measures applied by Xerox to satisfy the CC EAL2 assurance requirements.

Assurance Component	How requirement will be met
ACM_CAP.2 Configuration Items	The vendor provided configuration management documents and a Configuration Item list.
ADO_DEL.1 Delivery Procedures	The vendor provided delivery procedures.

Assurance Component	How requirement will be met
ADO_IGS.1 Installation, Generation and Startup procedures	The vendor provided secure installation, generation and start up procedures.
ADV_FSP.1 Informal function specification	The vendor provided an informal function specification.
ADV_HLD.1 Descriptive high-level design	The vendor provided a descriptive high-level design document.
ADV_RCR.1 Informal correspondence demonstration	The informal correspondence demonstration is provided in the design documentation. ST to FSP in the FSP, FSP to HLD in the HLD.
AGD_ADM.1 Administrator Guidance	The vendor submitted a system administration manual.
AGD_USR.1 User Guidance	The vendor submitted a user guide.
ATE_COV.1 Evidence of coverage	The analysis of test coverage was submitted in the evaluation evidence.
ATE_FUN.1 Functional testing	The test evidence was submitted to the CCTL.
ATE_IND.2 Independent testing – sample	The laboratory used development evidence submitted by the vendor along with functional testing evidence as a baseline for an independent test plan.
AVA_SOF.1 Strength of Function	The vendor submitted an analysis of the SOF for the PIN.
AVA_VLA.2 Independent vulnerability analysis	The vendor submitted vulnerability analysis was confirmed. The laboratory conducted an independent vulnerability assessment by building on the vendor's. The laboratory conducted penetration testing.

7 PROTECTION PROFILE (PP) CLAIMS

73 The TOE does not claim conformance to a PP.

8 RATIONALE

74 This section demonstrates the completeness and consistency of this ST by providing justification for the following:

Traceability — The security objectives for the TOE and its environment are explained in terms of threats countered and assumptions met. The SFRs are explained in terms of objectives met by the requirement. The traceability is illustrated through matrices that map the following:

- security objectives to threats encountered
- environmental objectives to assumptions met
- SFRs to objectives met

Assurance Level — A justification is provided for selecting an EAL2 level of assurance for this ST.

SOF — A rationale is provided for the SOF level chosen for this ST.

Dependencies — A mapping is provided as evidence that all dependencies are met.

8.1 Security Objectives Rationale

75 This section demonstrates that all security objectives for the TOE are traced back to aspects of the identified threats to be countered and/or aspects of the organizational security policies to be met by the TOE.

Table 9: Security Objectives Rationale

Objective	Threat Organizational Security Policy Assumption	Rationale
O.RESIDUAL	T.RECOVER	O.RESIDUAL helps to counter the threat T.RECOVER by limiting the amount of time that temporary document image data is on the hard disk drives or drive. By removing this temporary data, the window of opportunity is reduced to the time necessary to process the job. The TSF_IOWN and TSF_IOWC functions overwrite any residual data as described in DoD 5200.28-M.
O.MANAGE	T.RECOVER	The O.MANAGE objective helps to counter the threat T.RECOVER by ensuring that the TOE is

Objective	Threat Organizational Security Policy Assumption	Rationale
		properly configured and operating in accordance with stated security guidance.
O.ONDEMAND	T.RECOVER	O.ONDEMAND helps counter the threat T.RECOVER because by manually invoking the image overwrite (ODIO) function, the system administrator is able to minimize the opportunity an adversary has to access temporary document image data on the HDD(s) from print, scan to email, network scan, network fax, or copy jobs on the MFD and from copy jobs on the DC. O.ONDEMAND also helps counter the threat T.RECOVER when the device is decommissioned or moved. By manually invoking the image overwrite function, the system administrator is able to sanitize the HDDs before the device is taken out of service.

Table 10: Security Objectives Rationale for the Non-IT Environment

Objective	Threat Organizational Security Policy Assumption	Rationale
OE.MANAGE	A.CHANGE_KOC A.INSTALL A.MANAGE A.NO_EVIL_ADM A.PROCEDURE	OE.MANAGE is met by A.CHANGE_KOC, A.INSTALL, A.MANAGE, A.NO_EVIL_ADM, A.PROCEDURE by providing a trustworthy and responsible person to oversee the installation, configuration and operation of the TOE, using a secure PIN changed at specified intervals.
OE.PHYSICAL	A.PHYSICAL_ PROTECT	OE.PHYSICAL is met by the A.PHYSICAL_ PROTECT environmental assumption. This assumption acknowledges the need for the TOE to be located within facilities providing controlled access to prevent unauthorized physical access to critical internal parts of the TOE, the TOE serial port, and/or the external HDD cabinet (if present).

8.2 Security Requirements Rationale

76 This section provides evidence that demonstrates that the security objectives for the TOE and the IT environment are satisfied by the security requirements.

77 These mappings demonstrate that all TOE security requirements can be traced back to one or more TOE security objective(s), and all TOE security objectives are supported by at least one security requirement.

8.2.1 Rationale For TOE Security Requirements

78 This section provides evidence demonstrating that the security objectives of the TOE are satisfied by the security requirements. The following paragraphs provide the security requirement to security objective mapping and a rationale to justify the mapping.

Table 11: Security Objectives Rationale for the Environment

SFR	Rationale
FDP_RIP.1 (1)	Ensures that residual temporary document data does not remain on the mass storage device once the corresponding job has completed processing (IIO) or when circumstances compel the system administrator to invoke ODIO. This SFR traces back and meets O.RESIDUAL and O.ONDEMAND.
FDP_RIP.1 (2)	Ensures that residual temporary document data does not remain on the mass storage device once the corresponding job has completed processing or when circumstances compel the system administrator to invoke ODIO. This SFR traces back and meets O.RESIDUAL and O.ONDEMAND.
FIA_UID.2	Ensures that system administrators are identified before accessing the security functionality of the TOE. This SFR traces back to and aids in meeting the following objective: O.MANAGE.
FIA_UAU.2	Ensures that system administrators are authenticated before accessing the security functionality of the TOE. This SFR traces back to and aids in meeting the following objective: O.MANAGE.
FIA_UAU.7	Ensures that only obscured feedback generated by the authentication process is provided to system administrators before successful authentication. This SFR traces back to and aids in meeting the following objective: O.MANAGE.
FMT_MOF.1	Ensures that only system administrators have the capability to enable or disable the IIO capability of TSF_IOWN and TSF_IOWC, change the system administrator PIN, and invoke or abort the ODIO capability of TSF_IOWN and TSF_IOWC. This SFR traces back and aids in meeting the following objectives: O.MANAGE and O.ONDEMAND.

SFR	Rationale
FMT_SMF.1	Ensures that critical security management functions (i.e., enable/disable IIO, change system administrator PIN, and invoke/abort ODIO) are available on the TOE. This SFR traces back and aids in meeting the following objectives: O.MANAGE and O.ONDEMAND.
FMT_SMR.1	Ensures that the TOE maintains the system administrator role – a trusted individual who can administer the TOE. This SFR traces back and aids in meeting O.MANAGE and O.ONDEMAND.

Table 12: TOE SFR Mapping to Objectives

	O.RESIDUAL	O.MANAGE	O.ONDEMAND
FDP_RIP.1	**X**		**X**
FIA_UAU.2		**X**	
FIA_UAU.7		**X**	
FIA_UID.2		**X**	
FMT_MOF.1		**X**	**X**
FMT_SMF.1		**X**	**X**
FMT_SMR.1		**X**	**X**

8.3 Rationale For Assurance Level

79 This ST has been developed for multi-function digital image processing and digital copier products incorporating an Image Overwrite Security option. The TOE will be exposed to a low level of risk because the TOE sits within office space to which access is controlled (e.g., employee-only space). In such a public space, an agent would not have the prolonged access necessary to physically remove the internal HDD(s) from the TOE nor would there be time for an agent to connect a device (e.g., laptop or notebook) to the TOE via the serial port, locate latent image data, and copy it without being discovered and challenged. Similarly, an agent without the barrel lock keys that secure each disk carrier in the removable HDD cabinet could not forcibly remove the drive(s) without attracting attention nor, given the more stringent security measures implemented in the type of high-security environment for which the this option is intended, would an agent be able to disconnect the cabinet and remove it from the facility without being challenged. Therefore, Evaluation Assurance Level 2 is appropriate.

8.4 Rationale For TOE Summary Specification

80 This section demonstrates that the TSFs and Assurance Measures meet the SFRs.

81 The specified TSFs work together to satisfy the TOE SFRs. Table 13 provides a mapping of SFRs to the TSFs to show that each SFR is captured within a security function.

Table 13: Mapping of SFRs to Security Functions

SFR	Name	TSF	Name
FDP_RIP.1 (1)	Subset Residual Information Protection	TSF_IOWN	Image Overwrite Network Controller
FDP_RIP.1 (2)	Subset Residual Information Protection	TSF_IOWC	Image Overwrite Copy Controller
FIA_UAU.2	User Authentication before any Action	TSF_AUT	Authentication
FIA_UAU.7	Protected Authentication Feedback	TSF_AUT	Authentication
FIA_UID.2	User identification before any action	TSF_AUT	Authentication
FMT_MOF.1	Management of Security Functions Behavior	TSF_FMT	Security Management
FMT_SMF.1	Specification of Management Functions	TSF_FMT	Security Management
FMT_SMR.1	Security Roles	TSF_FMT	Security Management
FMT_SMR.1	Security Roles	TSF_AUT	Authentication

8.4.1 TOE Assurance Requirements

82 Section 6.2 of this document identifies the Assurance Measures implemented by Xerox to satisfy the assurance requirements of EAL2 as delineated in the table in Annex B of the CC, Part 3. Table 14 maps the Assurance Requirements with the Assurance Measures as stated in Section 5.2.

Table 14: Assurance Measure Compliance Matrix

Assurance Measure	Configuration Management	Delivery and Operation	Development	Guidance	Test	Vulnerability Assessment
ACM_CAP.2	**X**					
ADO_DEL.1		**X**				
ADO_IGS.1		**X**				

Assurance Measure	Configuration Management	Delivery and Operation	Development	Guidance	Test	Vulnerability Assessment
ADV_FSP.1			X			
ADV_HLD.1			X			
ADV_RCR.1			X			
AGD_ADM.1				X		
AGD_USR.1				X		
ATE_COV.1					X	
ATE_FUN.1					X	
ATE_IND.2					X	
AVA_SOF.1						X
AVA_VLA.1						X

8.4.2 TOE SOF Claims

83 The overall TOE SOF claim is SOF-basic because this SOF is sufficient to resist the threats identified in Section 3.2. Section 8.1 provides evidence that demonstrates that TOE threats are countered by the TOE security objectives. Sections 8.2.1 and 8.2.2 demonstrate that the security objectives for the TOE and the TOE environment are satisfied by the security requirements. The SOF-basic claim for the TOE applies because the TOE protects against an unskilled attacker with no special tools from accessing the TOE. System administrator PINs are changed either every 40 days (8-digit PIN) or annually (9-digit PIN).

8.5 Rationale For SFR and SAR Dependencies

84 Table 15 is a cross-reference of the functional components, their related dependencies, and whether the dependency was satisfied.

Table 15: SFR Dependencies Status

Functional Component ID	Functional Component Name	Dependency (ies)	Satisfied
FDP_RIP.1 (1)	Residual Information Protection	None	
FDP_RIP.1 (2)	Residual Information Protection	None	
FIA_UAU.2	User Authentication before any Action	FIA_UID.1	Yes
FIA_UAU.7	Protected Authentication Feedback	FIA_UAU.1	Yes
FIA_UID.2	User identification before any action	none	
FMT_MOF.1	Management of Security Functions Behavior	FMT_SMF.1 FMT_SMR.1	Yes

Functional Component ID	Functional Component Name	Dependency (ies)	Satisfied
FMT_SMF.1	Specification of Management Functions	None	
FMT_SMR.1	Security Roles	FIA_UID.1	Yes

85 SAR dependencies identified in the CC have been met by this ST as shown in Table 16.

Table 16: EAL2 SAR Dependencies Satisfied

Assurance Component ID	Assurance Component Name	Dependencies	Satisfied
ACM_CAP.2	Configuration items	None	NA
ADO_DEL.1	Delivery procedures	None	NA
ADO_IGS.1	Installation, generation, and start-up procedures	AGD_ADM.1	YES
ADV_FSP.1	Informal functional specification	ADV_RCR.1	YES
ADV_HLD.1	Descriptive high-level design	ADV_FSP.1, ADV_RCR.1	YES
ADV_RCR.1	Informal correspondence demonstration	None	YES
AGD_ADM.1	Administrator guidance	ADV_FSP.1	YES
AGD_USR.1	User guidance	ADV_FSP.1	YES
ATE_COV.1	Evidence of coverage	ADV_FSP.1, ATE_FUN.1	YES
ATE_FUN.1	Functional testing	None	NA
ATE_IND.2	Independent testing-sample	ADV_FSP.1, AGD_ADM.1, AGD_USR.1, ATE_FUN.1	YES
AVA_SOF.1	Strength of TOE security function evaluation	ADV_FSP.1, ADV_HLD.1	YES
AVA_VLA.1	Developer vulnerability analysis	ADV_FSP.1, ATE_HLD.1 AGD_ADM.1, AGD_USR.1	YES

8.6 Rationale for Explicitly Stated Requirements

86 There are no explicitly stated requirements for the TOE.

8.7 Internal Consistency and Mutually Supportive Rationale

87 The set of security requirements provided in this ST form a mutually supportive and internally consistent whole for the following reasons:

a) The choice of security requirements is justified as shown in Sections 8.3 and 8.4. The choice of SFRs and SARs is based on the assumptions about the objectives for, and the threats to, the TOE and the security environment. This ST provides evidence that the security objectives counter threats to the TOE, and that physical, personnel, and procedural assumptions are satisfied by security objectives for the TOE environment.

b) The security functions of the TOE satisfy the SFRs as shown in Table 13. All SFR and SAR dependencies have been satisfied or rationalized as shown in Table 15 and Table 16 and described in Section 8.5.

c) The SARs are appropriate for the assurance level of EAL2 and are satisfied by the TOE as shown in Table 14. EAL2 was chosen to provide a basic level of independently assured security with the assumption that products used in these environments will meet the security needs of the environment.

d) The SFRs and SARs presented in Section 5 and justified in Sections 8.3 and 8.4 are internally consistent. There is no conflict between security functions, as described in Section 2 and Section 6, and the SARs to prevent satisfaction of all SFRs.