Canon imageRUNNER 2200/2800/3300 Series Software Version iR2200N-USen50.06 with Security Kit B1 Security Target
June 28, 2004
Document No. F3-0504-001(2)

COACT, Inc.
Rivers Ninety Five
9140 Guilford Road, Suite G
Columbia, MD 21046-2587
Phone: 301-498-0150
Fax: 301-498-0855

COACT, Inc. assumes no liability for any errors or omissions that may appear in this document.

DOCUMENT INTRODUCTION

Prepared By:

COACT, Inc.
9140 Guilford Road, Suite G
Columbia, Maryland 21046-2587

Prepared For:

Canon U.S.A., Inc.
One Canon Plaza
Lake Success, New York 11042

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), the Canon imageRUNNER 2200/2800/3300 Series Software Version iR2200N-USen50.06 with Security Kit B1. This Security Target (ST) defines a set of assumptions about the environment, a list of threats that the product intends to counter, a set of security objectives, a set of security requirements, and the IT security functions provided by the TOE which satisfy the set of requirements.

REVISION HISTORY

Rev	Description
	June 23, 2004, initial release
1	June 25, 2004, removed document names
2	June 28, 2004, removed statement regarding “contents subject to change”

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ACRONYMS

CHAPTER 1

1 Security Target Introduction

This Security Target (ST) describes the objectives, requirements and rationale for the Canon imageRUNNER 2200/2800/3300 Series Software Version iR2200N-USen50.06 with Security Kit B1. The language used in this Security Target is consistent with the *Common Criteria for Information Technology Security Evaluation, Version 2.1*, the ISO/IEC JTC 1/SC27, *Guide for the Production of PPs and STs, Version 0.9* and all National Information Assurance Partnership (NIAP) interpretations through April 30, 2003. As such, the spelling of terms is presented using the internationally accepted English.

1.1 Security Target Reference

This section provides identifying information for the Canon imageRUNNER 2200/2800/3300 Series Software Version iR2200N-USen50.06 with Security Kit B1 Security Target by defining the Target of Evaluation (TOE).

1.1.1 Security Target Name

Canon imageRUNNER 2200/2800/3300 Series Software Version iR2200N-USen50.06 with Security Kit B1 Security Target, document number F3-0504-001(2), dated June 28, 2004.

1.1.2 TOE Reference

Canon imageRUNNER 2200/2800/3300 Series Software Version iR2200N-USen50.06 with Security Kit B1

1.1.3 Security Target Evaluation Status

This ST has been evaluated.

1.1.4 Evaluation Assurance Level

Functional and assurance claims conform to EAL3 (Evaluation Assurance Level 3) from the *Common Criteria for Information Technology Security Evaluation, Version 2.1*.

1.1.5 Keywords

Canon, Canon U.S.A., imageRUNNER, iR, 2200, 2800, 3300, copy, print, scan, fax, RIP, residual information protection, object reuse, overwrite, secure erase, complete erase.

1.2 TOE Overview

This Security Target defines the requirements for the Canon imageRUNNER 2200/2800/3300 Series Software Version iR2200N-USen50.06 with Security Kit B1 TOE. The TOE is the software that drives the imageRUNNER copier and contains the Complete Erase feature. During print, scan, fax, and copy job processing, the imageRUNNER stores images as files on the hard disk drive. There is a risk that these images could be disclosed during subsequent jobs. When activated, the Complete Erase feature completely overwrites files on the imageRUNNER Hard Disk Drive once they are no longer needed.

1.2.1 Security Target Organisation

Chapter 1 of this ST provides introductory and identifying information for the TOE.

Chapter 2 describes the TOE and provides some guidance on its use.

Chapter 3 provides a security environment description in terms of assumptions, threats and organisational security policies.

Chapter 4 identifies the security objectives of the TOE and of the Information Technology (IT) environment.

Chapter 5 provides the TOE security and functional requirements, as well as requirements on the IT environment.

Chapter 6 is the TOE Summary Specification, a description of the functions provided by the TOE to satisfy the security functional and assurance requirements.

Chapter 7 identifies claims of conformance to a registered Protection Profile (PP).

Chapter 8 provides a rationale for the security objectives, requirements, TOE summary specification and PP claims.

1.3 Common Criteria Conformance

The Canon imageRUNNER 2200/2800/3300 Series Software Version iR2200N-USen50.06 with Security Kit B1 Security Target conforms to the Common Criteria (CC) Version 2.1 functional requirements (Part 2) and assurance requirements (Part 3).

1.4 Protection Profile Conformance

The Canon imageRUNNER 2200/2800/3300 Series Software Version iR2200N-USen50.06 with Security Kit B1 Security Target does not claim conformance to any registered Protection Profile.

1.5 Document Conventions

The CC defines four operations on security functional requirements. The font conventions below identify the conventions for the operations defined by the CC.

Assignment: indicated with bold text

Selection: indicated with underlined text

Refinement: indicated with bold text and italics

Iteration: indicated with typical CC requirement naming followed by a number in parenthesis for each iteration (e.g., FMT_MOF.1 (1))

CHAPTER 2

2 TOE Description

This section describes the evaluation configuration (TOE) for the Canon imageRUNNER 2200/2800/3300 Series Software Version iR2200N-USen50.06 with Security Kit B1. It distinguishes the physical and logical boundaries of the TOE. It also describes the user types, highlights the assets and capabilities of the TOE, and defines the protection mechanisms and access rights to these assets.

2.1 Overview

The TOE is the software that drives the imageRUNNER copier and contains the Complete Erase feature. During print, scan, fax, and copy job processing, the imageRUNNER stores images as files on the hard disk drive. There is a risk that these images could be disclosed during subsequent jobs. When activated, the Complete Erase feature completely overwrites files on the imageRUNNER hard disk drive once they are no longer needed.

2.2 Hardware and Software Versions

The following table contains configurations required for operation of the TOE.

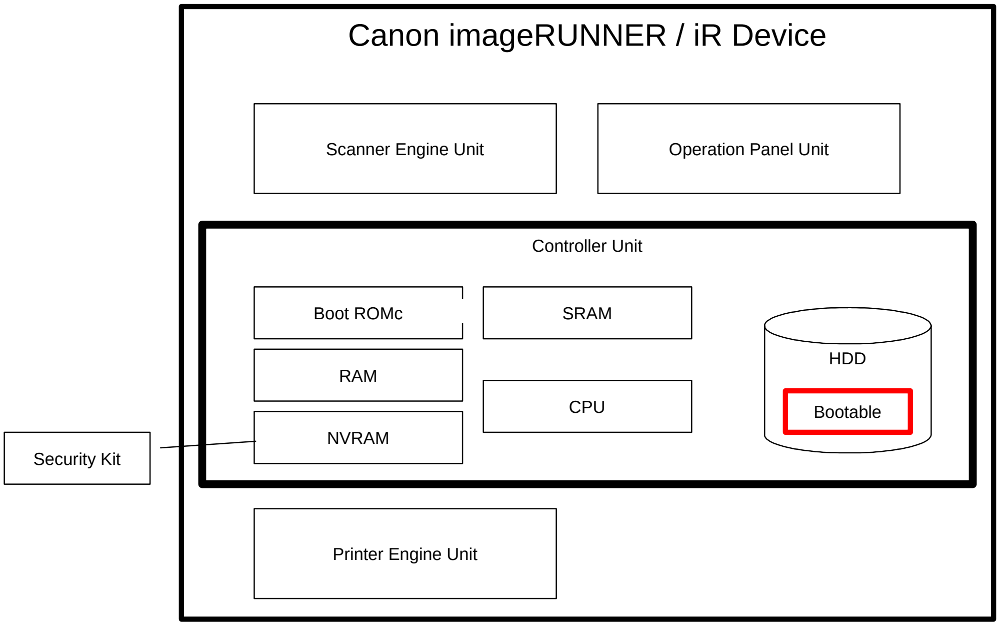
Table 1 - Hardware and Software Components

Component	Description
Bootable Version iR2200N-USen50.06	Software that controls all the functions of the imageRUNNER.
Security Kit B1	Tools and processes to replace the Bootable. The image in the kit has the Complete Erase functionality enabled.
imageRUNNER 2200/2800/3300 Series	Multifunction peripheral hardware device with scan, fax, print, and copy capabilities.

2.3 Architecture Description

The Canon imageRUNNER / iR Series is a multifunction peripheral device equipped with a large-size hard disk drive. It has scanning, printing, faxing, network, and digital image processing capabilities. By combining these functions, the imageRUNNER provides various application functions. Each of these functions involves storing image files on the hard drive.

Figure 1 - Canon imageRUNNER / iR Device Architecture



The Scanner Engine Unit consists of:

A) a mechanism for optical scanning that performs the scan function and,

B) an electronic device that obtains electronic image data by controlling the mechanism. The unit can both scan images and output scanned image data.

The Operation Panel Unit consists of:

A) a keypad for manipulating the imageRUNNER,

B) a display for interacting with users, and

C) other electronics to assist users. The unit can both receive input from users and show information on the display screen.

The Printer Engine Unit consists of:

A) a mechanism to provide electro-photographic printing, and

B) an electronic device to print out image data on paper by controlling the mechanism. The unit can receive image data input and produce printed images.

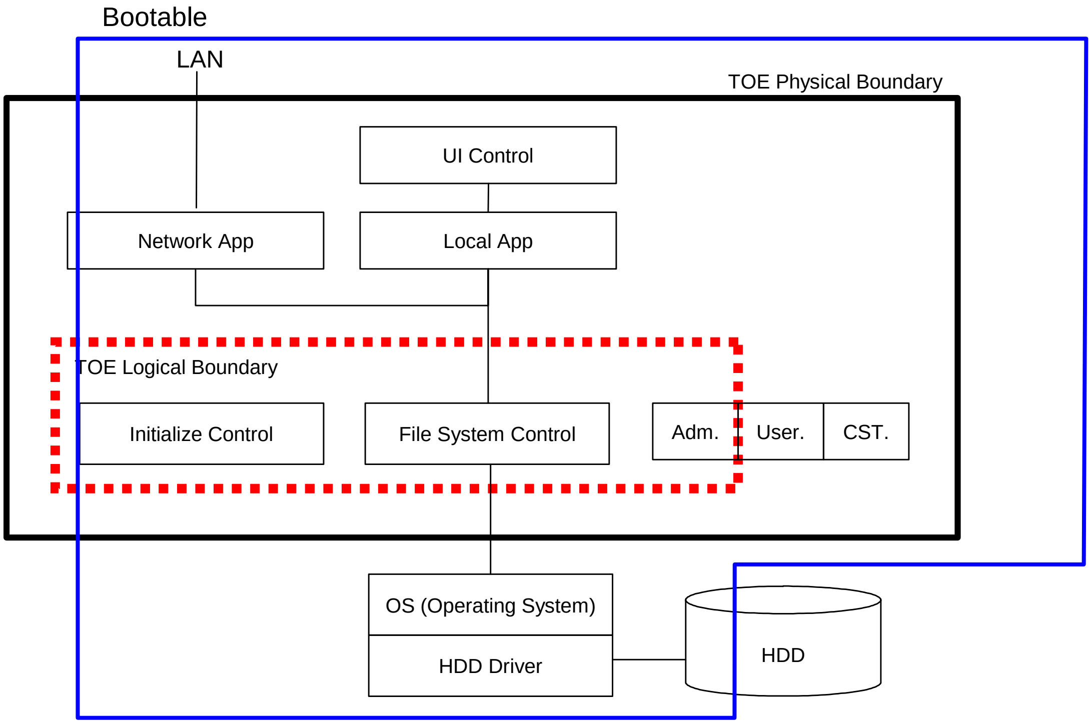
The Controller Unit controls all the functions of the Canon imageRUNNER and is composed of the following components in the table below. The Security Kit is an external piece of software used to activate and deactivate the Complete Erase function of the imageRUNNER. The assets protected by the TOE are the files stored on the hard drive.

Table 2 - Controller Components

Component	Description
Hard Disk Drive	A hard disk drive that physically stores image data, font data, log data as well as control information. A storage area of the hard disk drive holds the embedded software (Bootable).
CPU	The central processing unit of the Controller
RAM	Random access memory device providing volatile memory to the CPU
SRAM	Random access memory device providing battery supported memory in case of power loss
Boot ROM	A read only memory device that stores the startup instructions for the Controller and loads the Bootable
NVRAM	Non-volatile random access memory device that stores information that is not lost even in case of power loss, including function flags that control which features of the Controller are enabled

The software that drives the controller is called the Bootable. This software is a single software image that contains all the software that drives the imageRUNNER operation. Figure 2 below depicts the relation between the logical components that exist inside the Bootable.

Figure 2 - Canon imageRUNNER / iR Software Architecture



.

The UI control is a logical component that controls the LCD touch panel on the operation panel. The Network Application is a logical component that realizes the functions of printing via the network. The Local Application is a logical component that handles local image processing. The User component handles the role of an ordinary user of the system. The CST component provides the Canon Service Technician (CST) interface. The Admin component handles the role of an administrative user.

The File System is a logical component that provides file create, write, read, and delete interfaces to the other components. The delete function in the File System includes the logic to overwrite each file as it is deallocated. The Initialize Control handles system initialization and is the first code executed after the Bootable is loaded. The Initialise Control is responsible for overwriting any partially deleted files remaining on the hard drive after a power loss.

The Operating System (OS) component provides primitive operations for memory and hard disk drive access to the other components. The hard disk drive driver is a driver component that is used by the OS to access the disk drive.

The imageRUNNER architecture maintains a security domain for TOE execution that is protected from interference and tampering by untrusted subjects. The imageRUNNER is dedicated to providing copy, print, fax, and scan functions, and can not run any software other than the Bootable. The TOE security functions are contained in the Bootable, installed on the Controller, which can only be accessed by disassembling the machine. The entire Bootable represents a single executable.

The Complete Erase function is built into the fs_remove function within the File System control. Thus, all deallocations of files on the file system must invoke the fs_remove function and call the Complete Erase logic.

2.4 Physical Boundaries

The physical boundary of the TOE is the software in the Bootable of the Canon imageRUNNER 2200/2800/3300 Series Software Version iR2200N-USen50.06 with Security Kit B1 not including the Operating System or Hard Disk Driver, as shown in Figure 2 above.

2.5 Logical Boundaries

The logical boundary of the TOE is defined by the security features of the imageRUNNER as shown in Figure 2 above. The logical boundary includes the administrative interface to the Complete Erase feature and the implementation of that feature in the Initialize Control and File System Control.

The Complete Erase security feature ensures that image files on the file system are overwritten before that disk space is reused. Each time the imageRUNNER deletes a file from the file system, the disk space used by that file is overwritten.

The System Manager Logon feature ensures only authorized System Managers can access the security management functions of the imageRUNNER. Only users who are assigned as System Manager can activate or deactivate the Complete Erase function.

CHAPTER 3

3 TOE Security Environment

This chapter identifies assumptions (A), threats (T), and organisational security policies (P) related to the TOE. Assumptions are given to detail the expected environment and operating conditions of the system. Threats are those that are addressed by the TOE and operating environment. Organisational security policies are specific rules, procedures, or practices that are part of the TOE.

3.1 Threats

The threats identified in the following subsections are addressed by the TOE and IT environment, respectively.

3.1.1 Threats Addressed by the TOE

T.RESIDUAL An authorized user may receive residual information from a previous copy, print, fax, or scan job as the result of a TOE malfunction.

T.IMPERSONATE An unauthorized person gains access to TOE security management functions by impersonating an authorized System Manager.

3.1.2 Threats to be Addressed by the Operating Environment

TE.TAMPER An unauthorized person tampers with the TOE and accesses sensitive information from a previous copy, print, fax, or scan job.

3.2 Assumptions

The assumptions are ordered into three groups. They are personnel assumptions, physical environment assumptions, and IT environment assumptions.

Personnel assumptions describe characteristics of personnel who are relevant to the system.

Physical environment assumptions describe characteristics of the non-IT environment that the system is deployed in.

IT environment assumptions describe the technology environment that the TOE is operating within.

3.2.1 Personnel Assumptions

AE.NOEVIL System Managers are properly trained, follow all System Manager guidance, and do not attempt to attack or subvert the TOE and its policy.

AE.LOWTHREAT Attackers are assumed not to use sophisticated attack methods to attempt to compromise the TOE security functions.

3.2.2 Physical Environment Assumptions

AE.ENVIRON The physical environment of the TOE is sufficient for secure operation of the hardware.

AE.PHYSICAL The TOE cannot be physically accessed without disassembling the machine which embodies the TOE.

3.2.3 IT Environment Assumptions

AE.PLATFORM The hardware and software versions required by the TOE conform to the table in Section 2.2.

AE.OS The operating system and device drivers are the only way to access the file system and will correctly execute functions to read, write, and delete files.

AE.CORRECT The hardware and software required by the TOE are dedicated to the imageRUNNER and perform as documented for the TOE.

AE.ADMIN A competent System Manager will be assigned to manage the TOE and its security functions.

AE.INSTALL The hardware and software required by the TOE have been installed and configured according to the appropriate installation guides.

AE.CHANGE The System Manager password is changed at least every sixty (60) days.

3.3 Organisational Security Policies

No organisational security policies are required for the TOE security environment.

CHAPTER 4

4 Security Objectives

4.1 Security Objectives for the TOE

O.ERASE The TOE must completely overwrite image data when files are de-allocated.

O.ADMINAUTH The TOE must ensure that each System Manager is uniquely identified, and that the claimed identity is authenticated, before the System Manager is granted access to the TOE security management functions.

4.2 Security Objectives for the Operating Environment

OE.PHYSICAL The TOE cannot be physically accessed without disassembling the machine which embodies the TOE.

OE.NOTAMPER The TOE must be protected against external interference or tampering by untrusted subjects, or attempts by untrusted subjects to bypass the TOE security functions.

OE.LOWTHREAT The threat from System Managers and other users is considered low.

OE.CORRECT The hardware, operating system, and other software are dedicated to the TOE and function as documented for the TOE.

OE.MANAGE Documented procedures must exist for securely installing and administering the TOE.

4.3 Rationale for Security Objectives for the TOE

This section provides the rationale that all security objectives are traced back to aspects of the addressed threats.

O.ERASE O.ERASE addresses T.RESIDUAL because overwriting image data when files are deallocated ensures that the data can not be reused in subsequent jobs.

O.ADMINAUTH O.ADMINAUTH addresses T.IMPERSONATE as it ensures that people attempting to access TOE security management functions are first identified and authenticated.

Table 3 - Mappings Between Threats and Security Objectives for the TOE

	T.RESIDUAL	T.IMPERSONATE
O.ERASE	**X**	
O.ADMINAUTH		**X**

4.4 Rationale for Security Objectives for the Environment

This section provides the rationale that all security objectives for the environment are traced back to aspects of the addressed threats or assumptions.

OE.PHYSICAL	OE.PHYSICAL addresses AE.PHYSICAL because it ensures that an attacker cannot access the TOE without disassembling the machine.
OE.NOTAMPER	OE.NOTAMPER addresses TE.TAMPER because it ensures that there is no way to disable or bypass the Complete Erase or System Manager Logon functions.
OE.LOWTHREAT	OE.LOWTHREAT addresses AE.NOEVIL and AE.LOWTHREAT because it ensures that the threat from both administrators and other persons is low.
OE.CORRECT	OE.CORRECT addresses AE.PLATFORM, AE.OS, AE.CORRECT, and AE.INSTALL because it ensures that the hardware and operating system are properly built, accurately installed, and perform according to the documentation for the TOE.
OE.MANAGE	OE.MANAGE addresses AE.ENVIRON, AE.ADMIN, and AE.CHANGE because it ensures there are procedures in place for secure operation of the TOE in its environment.

Table 4 - Mappings Between Threats, Assumptions, and Security Objectives for the Environment

	AE.PHYSICAL	TE.TAMPER	AE.NOEVIL	AE.LOWTHRE	AE.ENVIRON	AE.PLATFOR	AE.OS	AE.CORRECT	AE.ADMIN	AE.INSTALL	AE.CHANGE
OE.PHYSICAL	**X**										
OE.TAMPER		**X**									
OE.LOWTHREAT			**X**	**X**							
OE.CORRECT						**X**	**X**	**X**		**X**	
OE.MANAGE					**X**				**X**		**X**

CHAPTER 5

5 IT Security Requirements

This section contains the security requirements that are satisfied by the TOE. These requirements consist of functional components from Part 2 of the CC and an Evaluation Assurance Level (EAL) containing assurance components from Part 3 of the CC.

The following table summarizes the security functional requirements claimed for the TOE and the IT Environment.

Table 5 - Security Functional Requirements

Security Functional Requirements	
FDP_RIP.1	Subset Residual Information Protection
FIA_SOS.1	Verification of Secrets
FIA_UAU.1	Timing of Authentication
FIA_UID.1	Timing of Identification
FMT_MOF.1	Management of Security Functions Behaviour
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security Roles
FPT_RVM.1	Non-bypassability of the TSP
FPT_SEP.1	TSF Domain Separation

5.1 TOE Security Functional Requirements

The TOE security functional requirements for this Security Target consist of the following components from Part 2 of the CC.

5.1.1 User Data Protection (FDP)

5.1.1.1 FDP_RIP.1 Subset Residual Information Protection

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the <u>deallocation of the resource from</u> the following objects: **file system**.

5.1.2 Identification and Authentication (FIA)

5.1.2.1 FIA_SOS.1 Verification of Secrets

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet **a length of seven digits, each digit in the range from 0 to 9 inclusive**.

5.1.2.2 FIA_UAU.1 Timing of Authentication

FIA_UAU.1.1 The TSF shall allow **copy, print, fax, scan** on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: FIA_UID.1 Timing of Identification

5.1.2.3 FIA_UID.1 Timing of Identification

FIA_UID.1.1 The TSF shall allow **copy, print, fax, and scan** on behalf of the user to be performed before the user is identified.

FIA_UID1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

5.1.3 Security Management (FMT)

5.1.3.1 FMT_MOF.1 Management of Security Functions Behaviour

FMT_MOF.1.1 The TSF shall restrict the ability to <u>disable, enable</u> the functions **Complete Erase** to **System Manager**.

Dependencies: FMT_SMF.1 Specification of Management Functions

FMT_SMR.1 Security Roles

5.1.3.2 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: **disable, enable the Complete Erase capability.**

5.1.3.3 FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles **System Manager**.

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

Dependencies: FIA_UID.1 Timing of Identification

5.2 IT Environment Security Functional Requirements

The IT Environment security functional requirements for this Security Target consist of the following components from Part 2 of the CC.

5.2.1 Protection of the TSF (FPT)

5.2.1.1 FPT_RVM.1 Non-bypassability of the TSP

FPT_RVM.1.1 The ***IT environment*** shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

5.2.1.2 FPT_SEP.1 TSF Domain Separation

FPT_SEP1.1 The ***IT environment*** shall maintain a security domain for ***TSF*** execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The ***IT environment*** shall enforce separation between the security domains of subjects in the TSC.

5.3 Explicitly Stated Security Functional Requirements

The security functional requirements detailed in this section are explicitly stated requirements that identify security functional requirements that are not currently defined in Part 2 of the CC v2.1.

NONE.

5.4 TOE Security Assurance Requirements

The TOE meets the assurance requirements for EAL3 as defined by Part 3 of the CC. These assurance requirements are summarized in the following table.

Table 6 - Assurance Requirements

Assurance Class	Component ID	Component Title
Configuration Management	ACM_CAP.3	Authorisation Controls
Configuration Management	ACM_SCP.1	TOE CM Coverage
Delivery and Operation	ADO_DEL.1	Delivery Procedures
Delivery and Operation	ADO_IGS.1	Installation, Generation, and Start-Up Procedures
Development	ADV_FSP.1	Informal Functional Specification
Development	ADV_HLD.2	Security Enforcing High-Level Design
Development	ADV_RCR.1	Informal Correspondence Demonstration
Guidance Documents	AGD_ADM.1	Administrator Guidance
Guidance Documents	AGD_USR.1	User Guidance
Life Cycle Support	ALC_DVS.1	Identification of Security Measures
Tests	ATE_COV.2	Analysis of Coverage
Tests	ATE_DPT.1	Testing: High-Level Design
Tests	ATE_FUN.1	Functional Testing
Tests	ATE_IND.2	Independent Testing - Sample
Vulnerability Assessment	AVA_MSU.1	Examination of Guidance
Vulnerability Assessment	AVA_SOF.1	Strength of TOE Security Function Evaluation
Vulnerability Assessment	AVA_VLA.1	Developer Vulnerability Analysis

5.5 TOE Strength of Function Claim

The only probabilistic or permutational mechanism in the imageRUNNER is the password mechanism used to authenticate System Managers. The claimed minimum strength of function is SOF-basic. FIA_SOS.1 and FIA_UAU.1 are the only TOE security functional requirements that depend on this permutational function.

5.6 Rationale for TOE Security Functional Requirements

This section provides the rationale for the functional requirements and demonstrates how each security objective is enforced by the functional requirements.

FDP_RIP.1 FDP_RIP.1 supports O.ERASE because it ensures that objects are made unavailable after they are deallocated from the file system.

FIA_SOS.1 FIA_SOS.1 supports O.ADMINAUTH because it ensures a password length that will make brute force attacks difficult for the assumed threat level.

FIA_UAU.1 FIA_UAU.1 supports O.ADMINAUTH by ensuring that copy, print, fax, and scan are the only TSF-mediated action allowed before authentication. Therefore, TSF management functions can only be accessed after the System Manager is authenticated.

FIA_UID.1 FIA_UID.1 supports O.ADMINAUTH by ensuring that copy, print, fax, and scan are the only TSF-mediated action allowed before identification. Therefore, TSF management functions can only be accessed after the System Manager is identified.

FMT_MOF.1 FMT_MOF.1 supports O.ADMINAUTH by restricting all security management functions to the System Manager.

FMT_SMF.1 FMT_SMF.1 supports O.ADMINAUTH by listing Complete Erase as the only security management function.

FMT_SMR.1 FMT_SMR.1 supports O.ADMINAUTH by listing System Manager as the only security role.

The following table contains a mapping of the functional requirements and the security objectives each requirement enforces.

Table 7 - Mappings between Functional Requirements and Security Objectives for the TOE

	O.ERASE	O. ADMINAUTH
FDP_RIP.1	X	
FIA_SOS.1		X
FIA_UAU.1		X
FIA_UID.1		X
FMT_MOF.1		X
FMT_SMF.1		X
FMT_SMR.1		X

5.7 Rationale for TOE Security Assurance Requirements

EAL3 was chosen to provide a moderate level of independently assured security. The chosen assurance level is consistent with the postulated threat environment. Specifically, that the threat of malicious attacks is not greater than moderate and the product will have undergone a search for obvious flaws.

The TOE stresses assurance through vendor actions that are within the bounds of current best commercial practice. The TOE provides, primarily via review of vendor-supplied evidence, independent confirmation that these actions have been competently performed.

The general level of assurance for the TOE is:

A) Consistent with current best commercial practice for IT development and provides a product that is competitive against non-evaluated products with respect to functionality, performance, cost, and time-to-market.

B) The TOE assurance also meets current constraints on widespread acceptance, by expressing its claims against EAL3 from part 3 of the Common Criteria.

5.8 Rationale for IT Environment Security Requirements

This section lists the functional requirements levied on the environment and the security objectives satisfied by the environment that each requirement enforces.

FPT_RVM.1 FPT_RVM.1 supports OE.NOTAMPER by ensuring that the TSP is always invoked before printing occurs.

FPT_SEP.1 FPT_SEP.1 supports OE.NOTAMPER by ensuring that the TSF is protected against interference and tampering by untrusted subjects.

The following table contains a mapping of the functional requirements and the security objectives each requirement enforces.

Table 8 - Mappings between Functional Requirements and Security Objectives for the Environment

	OE.NOTAMPER
FPT_RVM.1	**X**
FPT_SEP.1	**X**

5.9 Rationale for IT Security Requirement Dependencies

The following table lists the claimed TOE and IT Environment security requirements are their dependencies. This section also contains a rational for any dependencies that are not satisfied.

Table 9 - Security Functional Requirements

SFR	Dependencies	Hierarchical To
FDP_RIP.1	None	None
FIA_SOS.1	None	None
FIA_UAU.1	FIA_UID.1	None
FIA_UID.1	None	None
FMT_MOF.1	FMT_SMF.1 FMT_SMR.1	None
FMT_SMF.1	None	None
FMT_SMR.1	FIA_UID.1	None
FPT_RVM.1	None	None
FPT_SEP.1	None	None

5.10 Rationale for Strength of Function Claim

The claimed minimum strength of function is SOF-basic. The system manager logon requirements in FIA_SOS.1 and FIA_UAU.1 contain a permutational function requiring a SOF analysis. SOF-basic is defined in CC Part 1 section 2.3 as: "A level of the TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential." The rationale for the chosen level is based on the low attack potential of the threat agents identified in this ST.

Authorized System Managers choose their own password numbers when initially authorized to use the system. A very conservative estimate of one second was selected as the length of time required to enter a user id and password into the imageRUNNER. Therefore, the password space is calculated as follows:

Password length: p = 7

Unique characters: c = 10

Seconds per attempt: s = 1

Average length of successful attack in days =

= (s * c^p seconds) / (2 * 60 * 60 * 24 seconds per day)

= (1 * 10^7) / (2 * 60 * 60 * 24) days

= 57 days

Using the approach detailed in the CEM Part 2 Annex B, the values for “Identifying Value” and "Exploiting Value" in Table B.3 for each factor were summed. Given the simplicity of a brute force attack, all the values are 0 except for the Exploiting Value for Elapsed Time (8) and Access to TOE (9) for a total of 17. As shown in Table B.4, values between 10 and 17 indicate the mechanism is sufficient for a SOF Rating of ‘Basic’, resistant to an attack potential of ‘Low’.

CHAPTER 6

6 TOE Summary Specification

6.1 TOE Security Functions

This section describes the security functions implemented by the TOE to meet the TOE SFRs.

6.1.1 Complete Erase

The default delivery of a Canon imageRUNNER system does not have the Complete Erase capability enabled. To enable Complete Erase, an authorized Canon Service Technician must apply Security Kit B1 which consists of a dongle known as the Protect Key Device, the iR Series Security System Setup Tool CD-ROM, and Security Kit Guide. The CD-ROM contains a software tool that can communicate with the TOE and an image of the Bootable with the Complete Erase function enabled. The Service Technician must connect a Windows PC running the software tool to the imageRUNNER, connect the Protect Key Device to the PC, and use the software tool to upload the new Bootable image. Once completed, the Protect Key Device and PC are no longer required.

With the new Bootable in place, the Service Technician must set the erasing mode. Once set, these modes can be reset only by an authorized Service Technician. There are three erasing modes available:

A) Erase mode 1: Write NULL data once

B) Erase mode 2: Write random data once

C) Erase mode 3: Write random data three times.

After the Service Technician is finished, normal operation of the imageRUNNER may presume. Thereafter, the System Manager can activate or deactivate the Complete Erase function using the System Manager interface.

When active, the Complete Erase security feature is invoked each time that a file is deallocated through the use of the fs_remove function. The fs_remove function is the only way to deallocate files from the hard disk. The feature ensures that the areas of the hard disk currently allocated to the file being removed are overwritten according to the erasing mode selected.

6.1.2 System Manager Logon

The System Manager Logon feature ensures that only authorized System Managers can access the interface used to activate and deactivate the Complete Erase function. The System Manager credentials, a seven digit password and a numeric user id, are set using the System Manager Settings user interface. Once set, the credentials can only be changed by an authorized System Manager.

The System Manager Logon feature is invoked before access to the Complete Erase feature settings is allowed. Entering invalid credentials results in a failed logon attempt and a redisplay of the logon screen after a one second delay.

6.1.3 Security Management

Once the System Manager successfully logs in to the administrative interface, the System Manager has the ability to activate or deactivate the Complete Erase functionality.

6.2 Security Assurance Measures and Rationale

The assurance measures provided by the TOE satisfy all of the assurance requirements listed in the following table, which provides a reference between each TOE assurance requirement and the related vendor documentation that satisfies each requirement.

Table 10 - Assurance Measures and Rationale

Assurance Component	Rationale
ACM_CAP.3	The following Configuration Management procedures are described in this documentation: Use of the CVS tool for revision control Use of documented procedures for product builds Use of documented procedures for product test Use of documented procedures for release to manufacturing Use of documented procedures for distribution to customers List of configuration items and evidence that they are maintained by the CVS tool.
ACM_SCP.1	The documentation contains lists of the items tracked by the CVS revision control tool. These items include the TOE implementation representation, design documentation, test documentation, user documentation, administrator documentation, and CM documentation.
ADO_DEL.1	This document includes descriptions of the process used to create distribution copies of the TOE and the procedures used to ensure consistent delivery of the TOE.
ADO_IGS.1	These documents describe the procedures necessary for secure installation, generation, and start-up of the TOE.
ADV_FSP.1	These documents provide the purpose and method of use of all external TSF interfaces and completely represent the TSF.
ADV_HLD.2	These documents describe the high level design. They contain a representation of the TSF in terms of subsystems, identifying the TSP-enforcing subsystems, and describe the security functions. All subsystem interfaces are identified and the externally visible ones are noted. The purpose and method of use of all interfaces to

Assurance Component	Rationale
	the TSF subsystems are described.
ADV_RCR.1	The correspondence between the TOE security functions and the high-level design subsystems is described in these documents.
AGD_ADM.1	Guidance to administrators is effectively supported by the listed documentation for this requirement.
AGD_USR.1	Guidance to non-administrative users is effectively supported by the listed documentation for this requirement.
ALC_DVS.1	These documents describe the security measures employed to protect the confidentiality and integrity of the TOE design and implementation and provide evidence that measures are used.
ATE_COV.2	These documents describe the functional and penetration tests performed and their results.
ATE_DPT.1	These documents describe the functional and penetration tests performed and their results.
ATE_FUN.1	These documents describe the functional and penetration tests performed and their results.
ATE_IND.2	These documents describe the functional and penetration tests performed and their results.
AVA_MSU.1	These documents describe the vulnerability analysis performed and the results of the analysis.
AVA_SOF.1	These documents include a strength of function analysis to support the SOF-basic claim. The analysis includes identifying the TOE password space and the probability of a password being compromised.
AVA_VLA.1	These documents describe the vulnerability analysis performed and the results of the analysis.

6.3 Rationale for TOE Security Functions

The following section provides a rationale supporting how each security function satisfies each Security Functional Requirement.

FDP_RIP.1	Residual Information Protection. The Complete Erase feature supports FDP_RIP.1 by ensuring that all previous information content associated with a file on the hard disk is overwritten upon the deallocation of the resource from the file system.

FIA_SOS.1 Specification of Secrets. The System Manager Logon feature supports FIA_SOS.1 by ensuring a seven character password length.

FIA_UAU.1 Timing of Authentication. The System Manager Logon feature supports FIA_UAU.1 by ensuring that administrators are authenticated before accessing security management features.

FIA_UID.1 Timing of Identification. The System Manager Logon feature supports FIA_UID.1 by ensuring that administrators are identified before accessing security management features.

FMT_MOF.1 Management of Security Functions Behaviour. The System Manager Logon feature supports FMT_MOF.1 by ensuring that only administrators can access security management features. And, the Security Management feature supports FMT_MOF.1 by describing the System Manager's ability to configure the Complete Erase feature.

FMT_SMF.1 Specification of Management Functions. The Security Management feature supports FMT_SMF.1 by describing the System Manager's ability to configure the Complete Erase feature.

FMT_SMR.1 Security Roles. The System Manager Logon feature supports FMT_SMR.1 by ensuring that the System Manager is the only security role.

The following table shows the mapping between the Security Functional Requirements and the security functions provided by the TOE, which are listed above.

Table 11 - Mapping of Functional Requirements to Security Functions

	Complete Erase	System Manager Logon	Security Management
FDP_RIP.1	**X**		
FIA_SOS.1		**X**	
FIA_UAU.1		**X**	
FIA_UID.1		**X**	
FMT_MOF.1		**X**	**X**

FMT_SMF.1			**X**
FMT_SMR.1		**X**	

6.4 Appropriate Strength of Function Claim

The identification and authentication mechanism includes a password-based authentication feature that is probabilistic. FIA_SOS.1 and FIA_UAU.1 are the only TOE security functional requirements that depend on this permutational function. The System Manager Logon security function is the only security function that depends on this permutational function.

The rationale for choosing SOF-basic is based on the low attack potential of threats identified in this ST. The security objectives provide probabilistic security mechanisms and the strength of function claim is satisfied by the password management features provided by the TOE.

CHAPTER 7

7 Protection Profile Claims

This chapter provides detailed information in reference to the Protection Profile conformance identification that appears in Chapter 1, Section 1.4 Protection Profile Conformance.

7.1 Protection Profile Reference

This Security Target does not claim conformance to any registered Protection Profile.

7.2 Protection Profile Refinements

This Security Target does not claim conformance to any registered Protection Profile.

7.3 Protection Profile Additions

This Security Target does not claim conformance to any registered Protection Profile.

7.4 Protection Profile Rationale

This Security Target does not claim conformance to any registered Protection Profile.

CHAPTER 8

8 Rationale

This Security Target does not claim conformance to any Protection Profiles.

8.1 Security Objectives Rationale

Sections 4.3 - 4.4 provide the security objectives rationale.

8.2 Security Requirements Rationale

Sections 5.6 - 5.10 provide the security objectives rationale.

8.3 TOE Summary Specification Rationale

Sections 6.2 - 6.4 provide the TSS rationale.

8.4 Protection Profile Claims Rationale

This Security Target does not claim conformance to any Protection Profiles