EFI Fiery System 6 or 6e Secure Erase Option

and

EFI Fiery System 7 or 7e Secure Erase Option

Security Target

Version 1.0

3 October 2006

Prepared for:
Electronics for Imaging, Inc.

303 Velocity Way
Foster City, CA 94404

Prepared By:
Science Applications International Corporation

Common Criteria Testing Laboratory

7125 Columbia Gateway Drive, Suite 300
Columbia, MD 21046

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1. Security Target Introduction

This section identifies the Security Target (ST) and Target of Evaluation (TOE) identification, ST conventions, ST conformance claims, and the ST organization. The TOE is the EFI Fiery System 6 or 6e Secure Erase Option and EFI Fiery System 7 or 7e Secure Erase Option provided by Electronics for Imaging, Inc.

The TOE provides the ability to overwrite print jobs and ensures no residual information remains upon deallocation of the resource.

The Security Target contains the following additional sections:

- Section 2 – Target of Evaluation (TOE) Description

  This section gives an overview of the TOE, describes the TOE in terms of physical and logical boundaries, and states the scope of the TOE.

- Section 3 – TOE Security Environment

  This section details the expectations (assumptions) of the environment, the threats that are countered by the TOE and the environment, and the organizational security policy that the TOE must fulfill.

- Section 4 – TOE Security Objectives

  This section details the security objectives of the TOE and the environment.

- Section 5 – IT Security Requirements

  This section presents the security functional requirements (SFR) for the TOE and the IT Environment that supports the TOE, and details the assurance requirements for EAL3 augmented with ALC_FLR.1.

- Section 6 – TOE Summary Specification

  This section describes the security functions represented in the TOE that satisfies the security requirements.

- Section 7 – Protection Profile Claims

  This section presents any protection profile claims.

- Section 8 – Rationale

  This section closes the ST with the justifications of the security objectives, requirements and TOE summary specifications as to their consistency, completeness, and suitability

1.1 Security Target, TOE and CC Identification

ST Title – EFI Fiery System 6 or 6e Secure Erase Option and EFI Fiery System 7 or 7e Secure Erase Option Security Target

ST Version – Version 1.0

ST Date – 3 October 2006

TOE Identification – EFI Fiery System 6 or 6e Secure Erase Option and EFI Fiery System 7 or 7e Secure Erase Option

CC Identification – Common Criteria for Information Technology Security Evaluation, Version 2.2, Revision 256, January 2004.

1.2 Conformance Claims

This TOE is conformant to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 2.2, Revision 256, January 2004.
    - Part 2 Conformant
- Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements, Version 2.2, Revision 256, January 2004.
    - Part 3 Conformant
    - EAL 3 augmented with ALC_FLR.1

1.3 Conventions, Terminology, Acronyms

This section specifies the formatting information used in the Security Target.

1.3.1 Conventions

The following conventions have been applied in this document:

- Security Functional Requirements – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.
    - Iteration: allows a component to be used more than once with varying operations. In the ST, iteration is indicated by a letter in parenthesis placed at the end of the component. For example FDP_ACC.1a and FDP_ACC.1b indicate that the ST includes two iterations of the FDP_ACC.1 requirement, a and b.
    - Assignment: allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (e.g., [**assignment**]).
    - Selection: allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by brackets (e.g., [***selection***]).
    - Refinement: allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ **big** things …").
- Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as captions.

1.3.2 Terminology and Acronyms

The acronyms used within this Security Target:

ASIC	Application Specific Integrated Circuit
BIOS	Basic Input/Output System
Boot	To load the first piece of software that starts a computer, typically, the BIOS.
CMOS	Complementary metal oxide semiconductor
CPU	Central Processing Unit
CWPT	ColorWise Pro Tools
EAL	Evaluation Assurance Level
EEPROM	Electrically erasable programmable read-only memory

GUI	Graphical User Interface
HDD	Hard Disk Drive
IDE	Integrated Drive Electronics
I/O	Input/Output
LCD	Liquid Crystal Display
PCL	Printer Control Language
RIP	Raster Image Processing
SNMP	Simple Network Mail Protocol
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy

2. TOE Description

The Target of Evaluation (TOE) is the EFI Fiery System 6 or 6e Secure Erase Option and EFI Fiery System 7 or 7e Secure Erase Option software. The TOE provides the option to securely overwrite print job images. The Secure Erase Option contains the instructions to overwrite the images three (3) times when these print job images are no longer needed.

The Fiery System (the product) is installed on a machine running either Microsoft Windows XP Embedded or Linux operating systems. The version of the Fiery System (the product), which includes the TOE that runs on Microsoft Windows XP Embedded operating system, is referred to as the EFI Fiery System 6 and the EFI Fiery System 7. The version of the Fiery System (the product), which includes the TOE that runs on Linux operating system is referred as the EFI Fiery System 6e and the EFI Fiery System 7e.

During operation, images of print jobs submitted for printing are stored on the hard drive. The TOE will delete print job images left over from a completed print job by overwriting the sectors occupied by that image file with three (3) passes. The first pass overwrites the print job image with all zeros. The next pass overwrites the print job image with all ones. The final pass overwrites the print job image with random characters.

To activate or deactivate the secure erase option feature, the user must have administrator rights to the Fiery administrative screens. The IT Environment performs identification and authentication of all users to ensure they have the appropriate privileges (role) to access the TOE and its functions.

Figure 1 depicts the Fiery System product, including the TOE, the EFI Fiery System 6 or 6e Secure Erase Option and EFI Fiery System 7 or 7e Secure Erase Option. Within the Fiery System product, the major components are administrative management options, operator options, user options, secure erase option (the TOE), job management, color management, networking, and image rasterization.

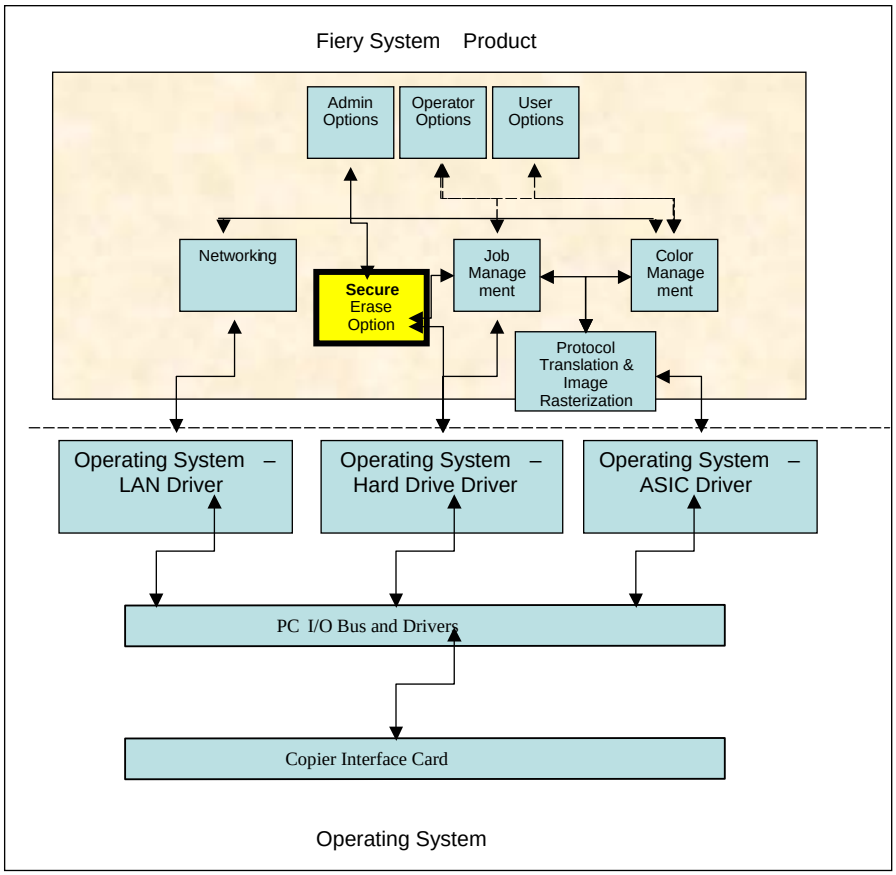

Figure 1 Fiery System Product Architecture

The following table provides a description of the major components of a print server.

Print Server Components	
EFI Fiery System 6 or 6e Secure Erase Option and EFI Fiery System 7 or 7e Secure Erase Option (TOE)	TOE - Software providing algorithm to overwrite deleted image files with random data.
EFI Fiery System Product	IT Environment – Software to manage the print server, which includes the following major components; administrative management options, operator options, user options, secure erase option (the TOE), job management, color management, networking, and image rasterization
Operating System	IT Environment - Software to control the computer hardware, drivers, and user interfaces
CPU	IT Environment - Intel brand Central Processing Unit
RAM	IT Environment - Random access memory providing temporary memory storage for computing functions
Motherboard, I/O Bus and Devices	IT Environment - Motherboard and common communications channel for hardware devices. I/O devices includes DVD/CD-ROM, Monitor/Keyboard
Hard drive (disk)	IT Environment - Physical storage holding operating system, Fiery software, TOE software, and user data
ASIC	IT Environment - ASIC containing compression algorithms
Copier Interface Card	IT Environment - Interface card containing physical port that will be connecting to the copier cable

Table 1 Print Server Hardware and Software Component Descriptions

Print jobs are submitted through two methods: over a LAN or imported locally from the hard drive. Once the print job is imported, processed, and marked for deletion, the TOE will delete the file (print job image) using the three-pass overwrite method (described above). If the TOE is not enabled, then the file is deleted by the standard operating system deletion method. The Windows and Linux operation deletion scheme is the removal of the file pointer to the space on the hard drive without erasing the actual data on the occupied hard drives sectors.

The only user of the TOE is the authorized administrator. The authorized administrator may modify options in the product to include the activation or deactivation of the TOE. However, for the TOE to be in the evaluated configuration, the overwrite feature must be enabled.

2.1.1 Physical Boundary

The physical boundary of the TOE is the EFI Fiery System 6 or 6e Secure Erase Option and EFI Fiery System 7 or 7e Secure Erase Option, which does not include the EFI Fiery System Product, the underlying operating system, the print server hardware, or hard disk as shown in Figure 1.

Following is a list of supported Fiery products that include the TOE.

System 6 Server	
Marketing Product Name	**Required Patches**
Fiery EXP8000 v1. 1J and EXP8000 v1.1JSP1 Color Server	1-OXED0
Fiery SP4000 Color Server	1-OWLFD
Fiery EXP250 Color Server	1-OWLF6
Fiery EXP6000 Color Server	1-JXWMS w/patch 1-OXECT
Fiery EXP5000 Color Server	1-OWPFO
ColorPass Z7100	1-OXAZ4
ColorPass Z6100	1-OXAZ4
ColorPass Z7500	1-OXAZ4
Fiery S300 / IP-901 Color Server	1-OYTWD
Fiery S450 / IC-302 Color Server	1-OXAYR
Fiery S300 50C-K / Fiery ES300 Color Server	1-OXAYX
System 6e	
Marketing Product Name	**Required Patches**
ImagePASS-M3, Network Multi-PDL Printer Unit-M3, PS Print Server PS-M3	1-OWL81
US: ImagePASS-S1 EFIGS: Network Multi PDL printer unit-S1 Japan: PS Print server unit-S1	1-OWL88
Fiery X3eTY 35C-KM / IC-402 Network Controller	1-OWL8F
Fiery Network Controller for DocuColor 5065	1-OWL8M
Fiery Network Controller for DocuColor 240/250	1-OWL8T
Fiery Network Controller for Ricoh E-7000	1-OWL90
System 7 Server	
Marketing Product Name	**Required Patches**
Fiery QC5000 Color Server	1-OXDNV
Océ 1070C	SP1.5 (1-N15QJ) w/patch 1-OXC1I
Océ 970C	SP1.5 (1-N15QJ) & 1-OXC1O
Fiery EXP8000 Color Server	1-OWJKL
Fiery Q5000 Color Server for iGen3	1-NF67W with patch 1-OX6VD
Fiery XP70 Color Server	1-OWLF5
Fiery EXP4110 Color Server	1-OWLF5
Fiery Color Server for Ricoh E-8000	1-OWY00
System 7e	
Marketing Product Name	**Required Patches**
USA: Canon imagePASS-C2 Europe: Canon Color Network Printer Unit-C2 Japan: Canon PS Print Server Unit-C2	1-OWL7H
Europe: Canon Color Network Printer Unit-F2 Japan: Canon PS Print Server Unit-F2	1-OWL7H
USA: Canon imagePASS-G1 Europe: Canon Color Network Printer Unit-G1 Japan: Canon PS Print Server Unit-G1	1-OWL7H

2.1.2 Logical Boundary

The logical boundaries are the TOE security functions. These functions include User Data Protection and Security Management.

2.1.2.1 User data protection

The Secure Erase Option feature ensures that print job image files on the hard drive are overwritten before that disk space is reused. Refer to Section 6.1.1 User data protection for more information.

2.1.2.2 Security management

The TOE provides the authorized administrator with ability to configure the overwrite feature of the TOE. Refer to Section 6.1.2 Security management for more information.

2.2 TOE Documentation

The Fiery Color Server Job Management Guide describes how to install and administer the TOE. Refer to Section 6.2 TOE Security Assurance Measures for information about this and other documents associated with the TOE.

3. Security Environment

The TOE security environment describes the security aspects of the intended environment in which the TOE is to be used and the manner in which it is expected to be employed.

The statement of the TOE security environment defines the following:

- Threats that the TOE is designed to counter
- Assumptions about the intended environment of the TOE
- Organizational security policies which the TOE is designed to comply

3.1 Threats

T.ACCESS	An unauthorized user may gain access to the TOE security functions and attempt to modify its behavior.
T.PRINT-RESIDUAL	A user may receive residual information from a deleted print job.

3.2 Secure Usage Assumptions

3.2.1 Personnel Assumptions

A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.NOEVIL	The authorized Administrators are not willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.

3.2.2 Physical Assumptions

A.LOCATION	The product will be located within an environment that is sufficient for secure operation.

3.2.3 System Assumptions

A.SYSTEM	The hardware and software with the TOE have been delivered, installed, and setup in accordance with documented delivery and installation procedures.

3.3 Organizational Security Policies

P.MANAGE	The TOE must provide authorized administrators with utilities to effectively manage the security-related functions.

4. Security Objectives

This section identifies the security objectives of the TOE and its supporting environment. Note that all of the IT security objectives are directed at the TOE, while all of the non-IT security objectives are directed at the TOE's intended environment.

4.1 IT Security Objectives for the TOE

O.MANAGE	The TOE must allow administrators to effectively manage the TOE and its security functions, and must ensure that only authorized administrators are able to access such functionality.
O.NO-RESIDUAL-DATA	The TOE must ensure that a user's print job information is not made available to another user.

4.2 IT Security Objectives for the Environment

OE.AUTH	The IT Environment must ensure that only authorized administrators gain access to the TOE, functions, and resources by uniquely identifying and authenticating all users before granting access to the TOE, functions, and resources.
OE.ENV_ADMIN	The TOE operating environment must provide functions for the administrator to manage its security functions, and must ensure that only authorized administrators are able to access such functionality.

4.3 Non-IT Security Objectives for the Environment

OE.PERSON	Authorized administrators of the TOE shall be properly trained in the configuration and usage of the TOE and will follow the guidance provided. These users are not careless, negligent, or hostile.
OE.PHYSICAL	The environment in which the TOE operates is sufficient for secure operation.
OE.SYSTEM	The hardware and software with the TOE have been delivered, installed, and setup in accordance with the documented delivery and installation procedures

5. IT Security Requirements

This section defines the security functional requirements for the TOE as well as the security assurance requirements against which the TOE has been evaluated. All of the security requirements have been copied from version 2.2 of the applicable Common Criteria documents.

5.1 TOE Security Functional Requirements

The following table describes the SFRs that are candidates to be satisfied by EFI Fiery System 6 or 6e Secure Erase Option and EFI Fiery System 7 or 7e Secure Erase Option.

Requirement Class	Requirement Component
FDP: User data protection	FDP_RIP.1 Subset residual information protection
FMT: Security management	FMT_MOF.1: Management of security functions behavior
	FMT_SMF.1a: Specification of Management Functions

Table 2 TOE Security Functional Components

5.1.1 User data protection (FDP)

5.1.1.1 Subset residual information protection (FDP_RIP.1)

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [***deallocation of resources from***] the following objects: [**hard drive**].

5.1.2 Security management (FMT)

5.1.2.1 Management of security functions behavior (FMT_MOF.1)

FMT_MOF.1.1 The TSF shall restrict the ability to [***disable, enable***] the functions [**overwrite**] to [**Administrator**].

5.1.2.2 Specification of Management Functions (FMT_SMF.1a)

FMT_SMF.1a.1 The TSF shall be capable of performing the following security management functions: [**enable and disable overwrite feature**].

5.2 IT Environment Security Functional Requirements

The following table describes the SFRs that are candidates to be satisfied by IT Environment in which the TOE, EFI Fiery System 6 or 6e Secure Erase Option and EFI Fiery System 7 or 7e Secure Erase Option operates.

Requirement Class	Requirement Component
FIA: Identification and authentication	FIA_ATD.1: User attribute definition
	FIA_UAU.2: User authentication before any action
	FIA_UID.2: User identification before any action
FMT: Security management	FMT_MTD.1b: Management of TSF data
	FMT_SMF.1b: Specification of Management Functions
	FMT_SMR.1: Security roles

Table 3 IT Environment Security Functional Components

5.2.1 Identification and authentication (FIA)

5.2.1.1 User attribute definition (FIA_ATD.1)

FIA_ATD.1.1 The ~~TSF~~ **IT Environment** shall maintain the following list of security attributes belonging to individual users: **[authentication data (password), and role]**.

5.2.1.2 User authentication before any action (FIA_UAU.2)

FAU_UAU.2.1 The ~~TSF~~ **IT Environment** shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

5.2.1.3 User identification before any action (FIA_UID.2)

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

5.2.2 Security management (FMT)

5.2.2.1 Management of TSF data (FMT_MTD.1)

FMT_MTD.1.1 The ~~TSF~~ **IT Environment** shall restrict the ability to **[*modify*, *delete*, create, assign]** the **[authentication data]** to **[Administrator]**.

5.2.2.2 Specification of Management Functions (FMT_SMF.1b)

FMT_SMF.1b.1 The ~~TSF~~ **IT Environment** shall be capable of performing the following security management functions: [**manage users security attributes**].

5.2.2.3 Security roles (FMT_SMR.1)

FMT_SMR.1.1 The ~~TSF~~ **IT Environment** shall maintain the roles [**Administrator**].
FMT_SMR.1.2 The ~~TSF~~ **IT Environment** shall be able to associate users with roles.

5.3 TOE Security Assurance Requirements

The security assurance requirements for the TOE are the EAL3 augmented with ALC_FLR.1 components as specified in Part 3 of the Common Criteria. No operations are applied to the assurance components.

Requirement Class	Requirement Component
ACM: Configuration management	ACM_CAP.3: Authorisation controls
	ACM_SCP.1: TOE CM coverage
ADO: Delivery and operation	ADO_DEL.1: Delivery procedures
	ADO_IGS.1: Installation, generation, and start-up procedures
ADV: Development	ADV_FSP.1: Informal functional specification
	ADV_HLD.2: Security enforcing high-level design
	ADV_RCR.1: Informal correspondence demonstration
AGD: Guidance documents	AGD_ADM.1: Administrator guidance
	AGD_USR.1: User guidance
ALC: Life cycle support	ALC_DVS.1: Identification of security measures
	ALC_FLR.1: Basic flaw remediation
ATE: Tests	ATE_COV.2: Analysis of coverage
	ATE_DPT.1: Testing: high-level design
	ATE_FUN.1: Functional testing
	ATE_IND.2: Independent testing - sample
AVA: Vulnerability assessment	AVA_MSU.1: Examination of guidance
	AVA_SOF.1: Strength of TOE security function evaluation
	AVA_VLA.1: Developer vulnerability analysis

Table 4 EAL 3 augmented with ALC_FLR.1 Assurance Components

5.3.1 Configuration management (ACM)

5.3.1.1 Authorisation controls (ACM_CAP.3)

ACM_CAP.3.1d The developer shall provide a reference for the TOE.
ACM_CAP.3.2d The developer shall use a CM system.
ACM_CAP.3.3d The developer shall provide CM documentation.
ACM_CAP.3.1c The reference for the TOE shall be unique to each version of the TOE.
ACM_CAP.3.2c The TOE shall be labelled with its reference.
ACM_CAP.3.3c The CM documentation shall include a configuration list and a CM plan.
ACM_CAP.3.4c The configuration list shall uniquely identify all configuration items that comprise the TOE.
ACM_CAP.3.5c The configuration list shall describe the configuration items that comprise the TOE.
ACM_CAP.3.6c The CM documentation shall describe the method used to uniquely identify the configuration items.
ACM_CAP.3.7c The CM system shall uniquely identify all configuration items.
ACM_CAP.3.8c The CM plan shall describe how the CM system is used.
ACM_CAP.3.9c The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.
ACM_CAP.3.10c The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.
ACM_CAP.3.11c The CM system shall provide measures such that only authorised changes are made to the configuration items.
ACM_CAP.3.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.1.2 TOE CM coverage (ACM_SCP.1)

ACM_SCP.1.1d The developer shall provide a list of configuration items for the TOE.
ACM_SCP.1.1c The list of configuration items shall include the following: implementation representation and the evaluation evidence required by the assurance components in the ST.
ACM_SCP.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.2 Delivery and operation (ADO)

5.3.2.1 Delivery procedures (ADO_DEL.1)

ADO_DEL.1.1d The developer shall document procedures for delivery of the TOE or parts of it to the user.
ADO_DEL.1.2d The developer shall use the delivery procedures.
ADO_DEL.1.1c The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.
ADO_DEL.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.2.2 Installation, generation, and start-up procedures (ADO_IGS.1)

ADO_IGS.1.1d The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.
ADO_IGS.1.1c The installation, generation and start-up documentation shall describe all the steps necessary for secure installation, generation and start-up of the TOE.
ADO_IGS.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADO_IGS.1.2e The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

5.3.3 Development (ADV)

5.3.3.1 Informal functional specification (ADV_FSP.1)

ADV_FSP.1.1d The developer shall provide a functional specification.
ADV_FSP.1.1c The functional specification shall describe the TSF and its external interfaces using an informal style.
ADV_FSP.1.2c The functional specification shall be internally consistent.
ADV_FSP.1.3c The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions and error messages, as appropriate.
ADV_FSP.1.4c The functional specification shall completely represent the TSF.
ADV_FSP.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADV_FSP.1.2e The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

5.3.3.2 Security enforcing high-level design (ADV_HLD.2)

ADV_HLD.2.1d The developer shall provide the high-level design of the TSF.
ADV_HLD.2.1c The presentation of the high-level design shall be informal.
ADV_HLD.2.2c The high-level design shall be internally consistent.
ADV_HLD.2.3c The high-level design shall describe the structure of the TSF in terms of subsystems.
ADV_HLD.2.4c The high-level design shall describe the security functionality provided by each subsystem of the TSF.
ADV_HLD.2.5c The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.
ADV_HLD.2.6c The high-level design shall identify all interfaces to the subsystems of the TSF.

ADV_HLD.2.7c The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

ADV_HLD.2.8c The high-level design shall describe the purpose and method of use of all interfaces to the subsystems of the TSF, providing details of effects, exceptions and error messages, as appropriate.

ADV_HLD.2.9c The high-level design shall describe the separation of the TOE into TSP-enforcing and other subsystems.

ADV_HLD.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_HLD.2.2e The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

5.3.3.3 Informal correspondence demonstration (ADV_RCR.1)

ADV_RCR.1.1d The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

ADV_RCR.1.1c For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

ADV_RCR.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.4 Guidance documents (AGD)

5.3.4.1 Administrator guidance (AGD_ADM.1)

AGD_ADM.1.1d The developer shall provide administrator guidance addressed to system administrative personnel.

AGD_ADM.1.1c The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

AGD_ADM.1.2c The administrator guidance shall describe how to administer the TOE in a secure manner.

AGD_ADM.1.3c The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

AGD_ADM.1.4c The administrator guidance shall describe all assumptions regarding user behaviour that are relevant to secure operation of the TOE.

AGD_ADM.1.5c The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

AGD_ADM.1.6c The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_ADM.1.7c The administrator guidance shall be consistent with all other documentation supplied for evaluation.

AGD_ADM.1.8c The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.

AGD_ADM.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.4.2 User guidance (AGD_USR.1)

AGD_USR.1.1d The developer shall provide user guidance.

AGD_USR.1.1c The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.

AGD_USR.1.2c The user guidance shall describe the use of user-accessible security functions provided by the TOE.

AGD_USR.1.3c The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.

AGD_USR.1.4c The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behaviour found in the statement of TOE security environment.

AGD_USR.1.5c The user guidance shall be consistent with all other documentation supplied for evaluation.
AGD_USR.1.6c The user guidance shall describe all security requirements for the IT environment that are relevant to the user.
AGD_USR.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.5 Life cycle support (ALC)

5.3.5.1 Identification of security measures (ALC_DVS.1)

ALC_DVS.1.1d The developer shall produce development security documentation.
ALC_DVS.1.1c The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.
ALC_DVS.1.2c The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.
ALC_DVS.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ALC_DVS.1.2e The evaluator shall confirm that the security measures are being applied.

5.3.5.2 Basic flaw remediation (ALC_FLR.1)

ALC_FLR.1.1d The developer shall provide flaw remediation procedures addressed to TOE developers.
ALC_FLR.1.1c The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.
ALC_FLR.1.2c The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.
ALC_FLR.1.3c The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.
ALC_FLR.1.4c The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.
ALC_FLR.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.6 Tests (ATE)

5.3.6.1 Analysis of coverage (ATE_COV.2)

ATE_COV.2.1d The developer shall provide an analysis of the test coverage.
ATE_COV.2.1c The analysis of the test coverage shall demonstrate the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.
ATE_COV.2.2c The analysis of the test coverage shall demonstrate that the correspondence between the TSF as described in the functional specification and the tests identified in the test documentation is complete.
ATE_COV.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.6.2 Testing: high-level design (ATE_DPT.1)

ATE_DPT.1.1d The developer shall provide the analysis of the depth of testing.
ATE_DPT.1.1c The depth analysis shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the TSF operates in accordance with its high-level design.
ATE_DPT.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.6.3 Functional testing (ATE_FUN.1)

ATE_FUN.1.1d The developer shall test the TSF and document the results.

ATE_FUN.1.2d The developer shall provide test documentation.
ATE_FUN.1.1c The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.
ATE_FUN.1.2c The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.
ATE_FUN.1.3c The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.
ATE_FUN.1.4c The expected test results shall show the anticipated outputs from a successful execution of the tests.
ATE_FUN.1.5c The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.
ATE_FUN.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.6.4 Independent testing - sample (ATE_IND.2)

ATE_IND.2.1d The developer shall provide the TOE for testing.
ATE_IND.2.1c The TOE shall be suitable for testing.
ATE_IND.2.2c The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.
ATE_IND.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ATE_IND.2.2e The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.
ATE_IND.2.3e The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

5.3.7 Vulnerability assessment (AVA)

5.3.7.1 Examination of guidance (AVA_MSU.1)

AVA_MSU.1.1d The developer shall provide guidance documentation.
AVA_MSU.1.1c The guidance documentation shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.
AVA_MSU.1.2c The guidance documentation shall be complete, clear, consistent and reasonable.
AVA_MSU.1.3c The guidance documentation shall list all assumptions about the intended environment.
AVA_MSU.1.4c The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls).
AVA_MSU.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AVA_MSU.1.2e The evaluator shall repeat all configuration and installation procedures to confirm that the TOE can be configured and used securely using only the supplied guidance documentation.
AVA_MSU.1.3e The evaluator shall determine that the use of the guidance documentation allows all insecure states to be detected.

5.3.7.2 Strength of TOE security function evaluation (AVA_SOF.1)

AVA_SOF.1.1d The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.
AVA_SOF.1.1c For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.
AVA_SOF.1.2c For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.

AVA_SOF.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AVA_SOF.1.2e The evaluator shall confirm that the strength claims are correct.

5.3.7.3 Developer vulnerability analysis (AVA_VLA.1)

AVA_VLA.1.1d The developer shall perform a vulnerability analysis.
AVA_VLA.1.2d The developer shall provide vulnerability analysis documentation.
AVA_VLA.1.1c The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for obvious ways in which a user can violate the TSP.
AVA_VLA.1.2c The vulnerability analysis documentation shall describe the disposition of obvious vulnerabilities.
AVA_VLA.1.3c The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.
AVA_VLA.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AVA_VLA.1.2e The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure obvious vulnerabilities have been addressed.

6. TOE Summary Specification

This chapter describes the security functions and associated assurance measures.

6.1 TOE Security Functions

Each of the security function descriptions is organized by the security requirements corresponding to the security function. Hence, each function is described by how it specifically satisfies each of its related requirements. This serves to both describe the security functions and rationalize that the security functions are suitable to satisfy the necessary requirements.

6.1.1 User data protection

FDP_RIP.1: Subset residual information protection

Before re-allocation of disk space, the sector level of the hard drive is overwritten multiple times (3) thereby ensuring no traces of print job image is left on the drive. The TOE ensures there is no residual information remaining on hard drive from the print jobs that have been queued, printed, and deleted.

The User Data Protection function is designed to satisfy the following security functional requirements:

- FDP_RIP.1: Subset residual information protection

6.1.2 Security management

FMT_MOF.1: Management of security functions behavior

The ability to manage the TOE is restricted to the authorized administrator. The authorized administrator is afforded the option to enable or disable the overwrite feature. However, in the evaluated configuration, the overwrite feature must always be enabled.

FMT_SMF.1: Specification of Management Functions

The TOE allows an authorized administrator enable and disable the overwrite feature to delete print job images.

The Security management function is designed to satisfy the following security functional requirements:

- FMT_MOF.1: Management of security functions behavior
- FMT_SMF.1: Specification of Management Functions

6.2 TOE Security Assurance Measures

6.2.1 Configuration management

The configuration management measures applied by EFI ensure that configuration items are uniquely identified, and that documented procedures are used to control and track changes that are made to the TOE. EFI ensures changes to the implementation representation are controlled. EFI performs configuration management on the TOE implementation representation, design documentation, tests and test documentation, user and administrator guidance, delivery and operation documentation, life-cycle documentation, vulnerability analysis documentation, and configuration management documentation.

These activities are documented in:

- Electronics for Imaging Software Configuration Management Plan (SCMP)
- EFI TOE Configuration Management Item Supplement

The Configuration management assurance measure satisfies the following EAL 3 augmented with ALC_FLR.1 assurance requirements:

- ACM_CAP.3
- ACM_SCP.1

6.2.2 Delivery and operation

EFI provides delivery documentation and procedures to identify the TOE, secure the TOE during delivery, and provide necessary installation and generation instructions. EFI's delivery procedures describe all applicable procedures to be used to prevent in appropriate access to the TOE. EFI also provides documentation that describes the steps necessary to install the TOE in accordance with the evaluated configuration.

These activities are documented in:

- Electronics for Imaging, Delivery Process Manual
- Release TO Manufacturing For Fiery Products, Guidelines to Define responsibilities and Milestone 45027243, Rev C
- Secure Erase Product Addendum for Fiery System 6/6e/7/7e OEM Specs (v1.5)

The Delivery and operation assurance measure satisfies the following EAL 3 augmented with ALC_FLR.1 assurance requirements:

- ADO_DEL.1
- ADO_IGS.1

6.2.3 Development

EFI has numerous documents describing all facets of the design of the TOE. In particular, they have a functional specification that describes the accessible TOE interfaces; a high-level design that decomposes the TOE architecture into subsystems and describes each subsystem and their interfaces; and, correspondence documentation that explains how each of the design abstractions correspond from the TOE summary specification in the Security Target to the subsystems.

These activities are documented in:

- Functional Specification:
    - Fiery System 6 Color Server Specification
    - Fiery System 6e (Color-Disk) Specification
    - Fiery Sys 7 Color Server Specification, EFI
    - Fiery System 7e (Color-Disk) Specification, EFI
    - Fiery System 6 Color Server Specification, Section 4
    - Secure Erase Product Addendum for Fiery System 6/6e/7/7e OEM Specs (v1.5)

- High-Level:
    - Fiery System 6 & 7 (Server) Secure Erase High Level Design Document
    - Fiery System 6e and 7e (Embedded) Secure Erase High Level Design Document

The Development assurance measure satisfies the following EAL 3 augmented with ALC_FLR.1 assurance requirements:

- ADV_FSP.1

- ADV_HLD.2
- ADV_RCR.1

6.2.4 Guidance documents

EFI provides administrator and user guidance on how to utilize the TOE security functions and warnings to administrators and users about actions that can compromise the security of the TOE.

These activities are documented in:

- Secure Erase Administrator Guide, version 1.2 March 22, 2006

The Guidance documents assurance measure satisfies the following EAL 3 augmented with ALC_FLR.1 assurance requirements:

- AGD_ADM.1
- AGD_USR.1

6.2.5 Life cycle support

EFI ensures the adequacy of the procedures used during the development and maintenance of the TOE through its life-cycle. EFI includes security controls on the development environment that are adequate to provide the confidentiality and integrity of the TOE design and implementation that is necessary to ensure the secure operation of the TOE. In addition, EFI identifies and tracks reported flaws, ensuring that they are addressed and corrections and corrective measures are made available as applicable

These activities are documented in:

- Electronics for Imaging Supplement Security Information, Version 1.0, May 2, 2005
- EFI Password Policy
- Electronics for Imaging Information Security Policy, Version 11.1, April 26, 2005
- Electronics for Imaging Corporate Headquarters Campus Security Protection
- Electronics for Imaging Security Procedures, Version 2005.1.0, February 28, 2005
- Information Technology Acceptable Use Policy for EFI Employees, Agents and Contractors
- Siebel Defect Process
- Defect resolution workflow
- EFI OEM Siebel Handbook

The Life cycle support assurance measure satisfies the following EAL 3 augmented with ALC_FLR.1 assurance requirements:

- ALC_DVS.1
- ALC_FLR.1

6.2.6 Tests

EFI has a test plan that describes how each of the necessary security functions is tested, along with the expected test results. EFI has documented each test as well as an analysis of test coverage and depth demonstrating that the security aspects of the design evident from the functional specification and high-level design are appropriately tested. Actual test results are also provided to demonstrate that the tests have been exercised and that the TOE operates as designed.

These activities are documented in:

- Network & Operating System Master Test Plan For Secure Erase Option, Version: 2.13, Date: March 8, 2006
- Network & Operating System Master Test Matrix Instructions For “Secure Erase Option (Embedded)”, Version: 0.67, Date: February 21, 2006
- Network & Operating System Master Test Matrix Instructions For “Secure Erase Option (Server)”, Version: 0.70, Date: February 21, 2005
- Actual Results for each product

The Tests assurance measure satisfies the following EAL 3 augmented with ALC_FLR.1 assurance requirements:

- ATE_COV.2
- ATE_DPT.1
- ATE_FUN.1
- ATE_IND.2

6.2.7 Vulnerability assessment

The TOE administrator and user guidance documents describe the operation of the TOE and how to maintain a secure state. These guides also describe all necessary operating assumptions and security requirements outside the scope of control of the TOE. They have been developed to serve as complete, clear, consistent, and reasonable administrator and user references.

The TOE does not identify any security functional requirements for which an explicit Strength of Function (SOF) is appropriate and does not identify any functions that are of a permutational or probabilistic nature. Therefore, a minimum SOF claim is not included for the TOE.

EFI performs regular vulnerability analyses of the entire TOE (including documentation) to identify obvious weaknesses that can be exploited in the TOE.

These activities are documented in:

- Secure Erase Product Addendum for Fiery System 6/6e/7/7e OEM Specs (v1.2)
- Fiery System 6/6e and 7/7e Secure Erase Vulnerability Assessment Document

The Vulnerability assessment assurance measure satisfies the following EAL 3 augmented with ALC_FLR.1 assurance requirements:

- AVA_MSU.1
- AVA_SOF.1
- AVA_VLA.1

7. Protection Profile Claims

There is no Protection Profile claim in this Security Target.

8. Rationale

This section provides the rationale for completeness and consistency of the Security Target. The rationale addresses the following areas:

- Security Objectives;
- Security Functional Requirements;
- Internal Consistency;
- Security Assurance Requirements;
- Strength of Functions;
- Requirement Dependencies;
- Explicitly Stated Requirements;
- TOE Summary Specification; and,
- PP Claims.

8.1 Security Objectives Rationale

This section provides a rationale for the existence of each assumption, threat, and organizational security policy statement. The following table demonstrates that the mapping between the assumptions, threats, and organizational security policy to the security objectives is complete. The discussion following provides the rationale of coverage for each assumption, threat, and organizational security policy.

8.1.1 Security Objectives Rationale for the TOE and Environment

This section provides evidence demonstrating the coverage of threats, organizational security policy, and usage assumptions by the security objectives.

	T.ACCESS	T.PRINT-RESIDUAL	A.MANAGE	A.NOEVIL	A.LOCATION	A.SYSTEM	P.MANAGE
O.MANAGE							X
O.NO-RESIDUAL-DATA		X					
OE.AUTH	X						
OE.ENV_ADMIN	X						
OE.PERSON			X	X			X
OE.PHYSICAL					X		
OE.SYSTEM						X	

Table 5 Environment to Objective Correspondence

8.1.1.1 T.ACCESS

An unauthorized user may gain access to the TOE security functions and attempt to modify its behavior.

This Threat is satisfied by ensuring that:

- OE.AUTH counters the threat by requiring each user be successfully identified and authenticated before any access to the TOE, functions, and resources is granted.
- OE.ENV_ADMIN the TOE operating environment counters the threat by ensuring the TOE operating environment provide functions for the administrator to manage its security functions, and ensures that only authorized administrators are able to access such functionality.

8.1.1.2 T.PRINT-RESIDUAL

A user may receive residual information from a prior print job.

This Threat is satisfied by ensuring that:

- O.NO-RESIDUAL-DATA counters the threat by ensuring that one users' print information is not made available to another user.

8.1.1.3 A.MANAGE

There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.

This Assumption is satisfied by:

- OE.PERSON ensures that the TOE is operated in a secure manner by competent, trained personnel, and they will abide by the guidance put forth. That they are not careless, negligent, or hostile.

8.1.1.4 A.NOEVIL

The authorized Administrators are not willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.

This Assumption is satisfied by:

- OE.PERSON ensures all authorized administrators are qualified and trained to manage the TOE.

8.1.1.5 A.LOCATION

The TOE will be located within an environment that is sufficient for secure operation.

This Assumption is satisfied by:

- OE.PHYSICAL ensures that the TOE is operated in an environment that is sufficient for secure operation.

8.1.1.6 A.SYSTEM

The hardware and software required by the TOE have been delivered, installed, and setup in accordance with documented delivery and installation procedures.

This Assumption is satisfied by:

- OE.SYSTEM ensures the hardware and software required by the TOE has been delivered, installed, and setup in accordance with documented delivery and installation procedures.

8.1.1.7 P.MANAGE

The TOE must provide authorized administrators with utilities to effectively manage the security-related functions of the system.

This Organizational Security Policy is satisfied by:

- O.MANAGE ensures there is a set of functions for administrators to use and that only authorized administrators have access to such functionality.
- OE.AUTH ensures each user is uniquely identified and authenticated prior to any TOE function accesses.
- OE.PERSON ensures competent administrators will manage the TOE.

8.1.2 Security Objectives for Non-IT Environment Rationale

The purpose for the Non-IT Environmental objectives is to provide protection for the TOE that cannot be addressed through IT measures. The defined objectives provide for physical protection of the TOE, proper management of the TOE, and interoperability requirements on the TOE. Together with the IT security objectives, these environmental objectives provide a complete description of the responsibilities of TOE in meeting security needs.

8.2 Security Requirements Rationale

This section provides evidence supporting the internal consistency and completeness of the components (requirements) in the Security Target. Note that the following table, Table 6 indicates the requirements that effectively satisfy the individual objectives.

8.2.1 Security Functional Requirements Rationale

All Security Functional Requirements (SFR) identified in this Security Target are fully addressed in this section and each SFR is mapped to the objective for which it is intended to satisfy.

	OE.AUTH	**OE.ENV_ADMIN**	**O.MANAGE**	**O.NO-RESIDUAL-DATA**
FDP_RIP.1				X
FIA_ATD.1	X			
FIA_UAU.2	X			
FIA_UID.2	X			
FMT_MOF.1			X	
FMT_MTD.1		X		
FMT_SMF.1a			X	
FMT_SMF.1b		X		
FMT_SMR.1		X		

Table 6 Objective to Requirement Correspondence

8.2.1.1 OE.AUTH

The TSF must ensure that only authorized administrators gain access to the TOE and its resources by uniquely identifying and authenticating all users before granting access to the TOE and its resources.

This TOE Security Objective is satisfied by ensuring that:

- FIA_ATD.1: define the unique attributes that are associated with individual users.

- FIA_UID.2: requires a user be successfully identified before any access to the TOE and TOE-protected resources is allowed.
- FIA_UAU.2: requires a user be successfully authenticated before any access to the TOE and TOE-protected resources is allowed.

8.2.1.2 OE.ENV_ADMIN

The TOE operating environment must provide functions for the administrator to manage its security functions, and must ensure that only authorized administrators are able to access such functionality.

This TOE Security Objective is satisfied by ensuring that:

- FMT_MTD.1: Restricts the ability to assign, create, delete, and/or modify the role security attribute that is assigned to an individual user to the authorized administrator.
- FMT_SMF.1b: Requires that the TOE provide the ability to manage its security functions including managing user attributes.
- FMT_SMR.1: The TOE maintains an administrator role.

8.2.1.3 O.MANAGE

The TOE must allow administrators to effectively manage the TOE and its security functions, and must ensure that only authorized administrators are able to access such functionality.

This TOE Security Objective is satisfied by ensuring that:

- FMT_MOF.1: Restricts the ability to disable and enable the overwrite feature to the authorized administrator.
- FMT_SMF.1a: Requires that the TOE provide the ability to manage its security functions including enabling and disabling the overwrite feature.

8.2.1.4 O.NO-RESIDUAL-DATA

The TOE must ensure that a user's print job information is not made available to another user.

This TOE Security Objective is satisfied by ensuring that:

- FDP_RIP.1: requires that when a print job is processed, the hard drive be overwritten multiple times (3), thereby ensuring no traces of data remains.

8.3 Internal Consistency Rationale

The ST includes no instance of a requirement that contradicts another requirement in the ST. In instances where different requirements apply to the same events or types of data, the requirements and the operations performed within the requirements do not contradict each other, but provide supporting functionality ensuring that the TOE is internally consistent.

The combination of several different supporting security functions and the inclusion of all dependencies as illustrated in Table 7 Requirement Dependency Rationale ensure that together the selected requirements form a mutually supportive whole. The following items also support this claim:

- Mapping and suitability of the requirements to security objectives (as justified in Table 6 Objective to Requirement Correspondence);
- Inclusion of identification and authentication to ensure only authorized users access the TOE functions and its data; and
- Inclusion of security management requirements to ensure proper configuration and control of other security functional requirements.

8.4 Security Assurance Requirements Rationale

This ST contains the assurance requirements from the CC EAL3 assurance package augmented with ALC_FLR.1. The EAL chosen is based on the statement of the security environment (assumptions and threats) and the security objectives defined in this ST. The sufficiency of the EAL chosen (EAL3 augmented with ALC_FLR.1) is justified based on those aspects of the environment that have impact upon the assurance needed in the TOE. The administrative staff is conscientious, non-hostile, and well trained (A.MANAGE and A.NOEVIL). The TOE is physically protected (OE.PHYSICAL) and is properly and securely configured (OE.SYSTEM). Given these aspects, a TOE based on good commercial development practices is sufficient and with the addition of flaw remediation procedures provide greater assurance that security-related bugs will be fixed in a widely distributed commercial product. EAL 3 is an appropriate level of assurance for the TOE described in this ST. As such, it is believed that EAL3 augmented with ALC_FLR.1 provides an appropriate level of assurance in the security functions offered by the TOE.

8.5 Strength of Functions Rationale

The TOE does not identify any security functional requirements for which an explicit Strength Of Function (SOF) is appropriate and does not identify any functions that are of a permutational or probabilistic nature. Therefore, a minimum SOF claim is not included for the TOE.

8.6 Requirement Dependency Rationale

The following table demonstrates that all dependencies among the claimed security requirements are satisfied and therefore the requirements work together to accomplish the overall objectives defined for the TOE.

ST Requirement	CC Dependencies	ST Dependencies
FDP_RIP.1	None	None
FIA_ATD.1	None	None
FIA_UAU.2	FIA_UID.1	FIA_UID.2
FIA_UID.2	None	None
FMT_MOF.1	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1a, FMT_SMR.1
FMT_MTD.1	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1b, FMT_SMR.1
FMT_SMF.1a-b	None	None
FMT_SMR.1	FIA_UID.1	FIA_UID.2

Table 7 Requirement Dependency Rationale

8.7 Explicitly Stated Requirements Rationale

There are no explicitly stated requirements in this Security Target.

8.8 TOE Summary Specification Rationale

Each subsection in Section 6, the TOE Summary Specification, describes a security function of the TOE. Each description is followed with rationale that indicates which requirements are satisfied by aspects of the corresponding security function. The set of security functions work together to satisfy all of the security functions and assurance requirements. Furthermore, all of the security functions are necessary in order for the TSF to provide the required security functionality.

This Section in conjunction with Section 6, the TOE Summary Specification, provides evidence that the security functions are suitable to meet the TOE security requirements. The collection of security functions work together to provide all of the security requirements. The security functions described in the TOE summary specification are all necessary for the required security functionality in the TSF. Table 8 Security Functions vs. Requirements Mapping demonstrates the relationship between security requirements and security functions.

	User data protection	Security management
FDP_RIP.1	X	
FMT_MOF.1		X
FMT_SMF.1		X

Table 8 Security Functions vs. Requirements Mapping

8.9 PP Claims Rationale

See Section 7, Protection Profile Claims.