EROTOE02

Innovation Data Processing

FDRERASE/OPEN Security Target

Version 1.0

January 24, 2008

Prepared for:
Innovation, Inc.

Innovation Plaza, 275 Patterson Avenue
Little Falls, NJ 07424-1658

Prepared By:
Science Applications International Corporation

Common Criteria Testing Laboratory

7125 Columbia Gateway Drive, Suite 300
Columbia, MD 21046

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 FDRERASE/OPEN provided by Innovation Data Processing, Inc. The TOE is an application and supporting operating system run on an x86 architecture computer system. The primary purpose of the TOE is to erase data from enterprise disk storage systems (i.e. large scale storage systems with one or more hard disks containing system and user data) that an organization may be scrapping or decommissioning, selling or returning, reusing for a different purpose within the organization or when an organization is leaving a recovery site, e.g., after a disaster recovery test, to prevent any access to any data that may reside on the disk storage system leaving their control. The TOE accomplishes erasure by overwriting, to destroy any data residing on the disk storage system making it no longer accessible. The disk erasure techniques provided by the TOE and described in this Security Target offer successively higher levels of data erasure security by overwriting once or, as appropriate, by overwriting multiple times using multiple data patterns and complements of those patterns, using suitable internal functions to insure data is physically written to disk and to confirm that erasure did take place.

The Security Target contains the following additional sections:

- TOE Description (Section 2)
- Security Environment (Section 3)
- Security Objectives (Section 4)
- IT Security Requirements (Section 5)
- TOE Summary Specification (Section 6)
- Protection Profile Claims (Section 7)
- Rationale (Section 8).

1.1 Security Target, TOE and CC Identification

ST Title – Innovation Data Processing FDRERASE/OPEN Security Target

ST Version – Version 1.0

ST Date – 24 January 2008

TOE Identification – Innovation Data Processing, FDRERASE/OPEN, Version 02, Level 05.

CC Identification – Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005.

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 2.3, August 2005.
    - Part 2 Extended
- Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements, Version 2.3, August 2005.
    - Part 3 Conformant
    - EAL 2 augmented with ALC_FLR.2

- Strength of Function Claim: SOF-basic.

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 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

CD-ROM	A non-volatile optical data storage medium using the same physical format as audio compact discs, readable by a computer with a CD-ROM (CDR) drive. The TOE employs an unalterable record-once format CD-ROM compact disc as a distribution media.
Channel	A general term used in place of the specific terms host adapter or host bus adapter (i.e. HBA), terms primarily used to refer to devices for connecting Fibre Channel and SCSI protocol devices to a host system (the computer) and other storage devices. It is a functional unit, controlled by the processor, which handles the transfer of data between processor storage and peripheral equipment. It contains error recovery logic.
channel programming interface	A software programming interface to a component of the operating system (e.g. disk driver) that enables the TOE to command the disk controller to perform I/O operations.
control unit	A device that coordinates and controls the operation of one or more input/output devices (such as a disk / hard disk) and synchronizes the operation of such devices with the operation of the system as a whole.
directory	An entity in a computer file system which describes the location, size and other characteristics of a group of files, programs and/or other directories, (also known as a catalog, folder or library.)
disk / hard disk	Non-volatile, digitally encoded data storage device that stores data on the magnetic surfaces of hard disk platters, (also known as HDD.)
disk storage	A category of data storage mechanisms for computers; where data is recorded on planar surfaces or 'disks' for temporary or permanent storage.
disk storage system	A storage system composed of a control unit, cache, a disk unit enclosure and one or more hard disks containing system and user data.

disk unit enclosure	A physical enclosure containing one or more disk units.
disk [volume]	The term used in place of the term "drive" where it is desirable to indicate that the entity in question may not be a physical hard disk drive (HDD), but rather the data stored on one or more disks using a filesystem. "Logical drive" and "volume" should be considered synonymous.
enterprise storage	The information technology focused on the storage, protection, and retrieval of data in large-scale environments. It is differentiated from consumer storage in many practical ways, ranging from the size of the environment to the technologies used.
error recovery software	Software particularly in the operating system that attempts to recover from I/O errors
executable (program)	A file whose contents are meant to be interpreted as a program by a computer.
functional unit	Hardware, software, or a combination of hardware and software that is capable of accomplishing a specified purpose.
GUI	A graphical user interface that allows a user to control and observe the TOE and/or an operator to control and observe the system operation
JAVA	A programming language that provides the ability to create a GUI for dialog services.
USB flash drive	A NAND-type flash memory data storage device integrated with a USB interface. They are typically small, lightweight, removable and rewritable.
library	A directory containing a collection of programs and subprograms used to develop software.
logical drive	The term used in place of the term "drive" where it is desirable to indicate that the entity in question is not a physical disk drive, but rather the data stored on one or more disks using a filesystem. Disk "volume" should be considered synonymous with "logical drive."
mount/unmount	To make a device available/unavailable for its normal intended use. A device (such as a disk volume) can also be described as being ‘on-line’ or ‘off-line’.
RAID	Redundant Array of Inexpensive Disks (or Redundant Array of Independent Disks), a data storage scheme using multiple hard drives to share or replicate data among the drives. The TOE is able to erase RAID systems.
release	A hardware command issued by the owning host bus adapter when a disk resource is taken offline; it frees a device for another host bus adapter to reserve.
reserve	A hardware command issued by a host bus adapter to obtain or maintain ownership of a device. A device that is reserved refuses all commands from all other host bus adapters except the one that initially reserved it, the initiator.
SATA	Serial Advanced Technology Attachment (SATA) is a computer bus primarily designed for transfer of data between a computer and storage devices (such as hard disk drives or optical drives). The TOE can erase SATA drives that have a controller that makes them appear to be SCSI drives. There are two types of controller that make ATA drives emulate SCSI drives: a Serial Attached SCSI (SAS) controller; and an Advanced Host Controller Interface (AHCI) SATA Controller operating in AHCI mode.
Volume [disk]	The term used in place of the term "drive" where it is desirable to indicate that the entity in question may not be a physical hard disk drive (HDD), but rather the data stored on one or more disks using a filesystem. "Logical drive" and "volume" should be considered synonymous.

Wikipedia maintains a Web site that contains base computer terminology, terms and definitions as well as the terminology used by many different vendors to describe their systems and products in one convenient location. To look up unfamiliar acronyms and terminologies go to: http://en.wikipedia.org/wiki/Main_Page

2. TOE Description

The Target of Evaluation (TOE) is Innovation Data Processing, FDRERASE/OPEN, Version 02 Level 05.

The TOE is an application and supporting operating system that runs on an x86 architecture computer. The function of the TOE is to erase data from the disks in a disk storage system (including RAID systems). The TOE also offers a capability to verify that user data has been erased.

2.1 TOE Overview

FDRERASE/OPEN is an application written in the C and JAVA programming languages. It is loaded onto a computer from a CD-ROM compact disc by a person authorized to possess that CD-ROM and an associated key device (USB flash drive). This person is acting in the role of "TOE Administrator". The CD-ROM containing FDRERASE/OPEN also contains a copy of the Sun Solaris 10 operating system, preconfigured to automatically start FDRERASE/OPEN after the boot of Solaris 10 is complete. This method results in Solaris 10 invoking FDRERASE/OPEN as the sole user application executing on the computer. The USB flash drive contains validation codes which match the CD-ROM. These codes are compared at startup. If they do not match, the TOE will exit. The USB flash drive is also used to store options, logs, and history records.

The TOE can erase any disk that is attached to its host computer by a SCSI or Fibre channel connection. The disks can be physical hard drives, or disk volumes resident in enterprise disk storage systems (including RAID systems) such as those provided by EMC, Hitachi, IBM, and other vendors.

The TOE is run by a person authorized to know the authentication data (i.e. authentication password) required to gain access to the TOE functions. This person is acting in the role of "TOE User". An authentication password at TOE start-up is a requirement to operate TOE in a manner that is consistent with CCEVS EAL2 certification prerequisites.

The "TOE User" controls the TOE using a GUI (graphic user interface) to select commands that direct the TOE as to what security function it is to perform.

There is no TOE requirement that a "TOE Administrator" and a "TOE User" be separate persons. A person with the privileges to possess the CD-ROM containing the TOE and the associated USB flash drive (i.e. "TOE Administrator") or to know the TOE authentication data (i.e., "TOE User"), is assumed to be trusted to perform the duties associated with those privileges. Any decision to require separation of these roles or not is left to the organizational management authority controlling the TOE site. Any person authorized to know the TOE authentication data is hereinafter referred to as the "TOE user".

The TOE provides two different levels of disk erasures. They are the ERASE and SECUREERASE functions. Disk erasures are actually performed by overwriting stored data to make the original data unrecoverable. This overwrite includes the disk directory. The TOE also provides a method to verify that user data has been erased. This is the VERIFY function.

- ERASE overwrites every sector of disk storage. The TOE writes an increment of sectors, with binary zeroes by default. This single overwrite will make all data originally on each sector unrecoverable by any normal program running anywhere that has direct access to the disk or through the disk control unit. Original data, however, may still be recoverable through sophisticated laboratory techniques and special programs whose purpose is to recover data on a disk by commanding the disk to skew read heads plus or minus a number of degrees. Any residual data recording on the "edge" of the sector may be recoverable using such a technique.

- SECUREERASE overwrites each disk sector a minimum of three times, writing a random pattern, a complement of the first pattern, and finally another random pattern, by default. This multiple overwrite process (optionally up to eight overwrites) makes the original data unrecoverable, even by sophisticated laboratory techniques applied to hard drives removed from the control unit.

- VERIFY function can be used to sample sectors on the erased volumes to ensure that they have been erased. By default it verifies a percentage of the volume but can verify the entire volume if needed.

The TOE provides administrative control and display control functions PRINT, TOGGLE, PAUSE, RESUME, CANCEL, DELETE TASK, and POWER DOWN. These functions do not interface directly to any security relevant functions. They interface only to administrative control and display control facilities.

- PRINT provides a way to display or view data residing on a disk. A formatted file is actually written to the FDRERASE/OPEN USB flash drive, which can then be printed if there is an attached printer, or printed later by plugging the USB flash drive into another computer running Windows, or any other operating system that will mount a USB flash drive. It should be noted that printing a great deal of data will probably fill up the USB flash drive.

  Warning: Care should be taken to ensure that persons authorized to use FDRERASE/OPEN are authorized to view all information stored on the disk storage systems to be erased.

- TOGGLE simply allows a user to 'toggle' between a single panel and a double panel display.

- DELETE is only valid against a task which is not yet started.

- PAUSE, RESUME, and CANCEL functions are performed on active tasks but they do not change the nature of the security function. The results of issuing a CANCEL function against an active SECUREERASE, ERASE or

- VERIFY security function will be displayed on the GUI and recorded in the log and history file output.

- POWER DOWN protects the integrity of the audit data in the logs and history file by synchronizes these files and prior the exit from the TOE application but again it does not change the action or result of a security function.

The TOE displays information on the progress of its various functions on the GUI. In addition, it records the results of its operations to log files that are stored on the USB flash drive.

The TOE supports enterprise disk storage systems from major manufacturers including IBM; EMC; and Hitachi.

2.2 TOE Architecture

2.2.1 Physical Components

The physical components of FDRERASE/OPEN comprise:

- CD/DVD containing the Solaris 10 Operating System and FDRERASE/OPEN application, in a locked state as well as the serial number of a specific corresponding USB flash drive.
- USB flash drive, with a serial number corresponding to the serial number recorded on the CD/DVD, that provides storage for audit logs, a history file and after installation[1] will contain the "FDRERASE/OPEN key".

2.2.2 IT Environment:

The intended FDRERASE/OPEN operating IT environment is an x-86 compatible computer, with a time of day clock (TOD) function, capable of supporting Solaris 10, located in a physically secure environment, and to which is connected by SCSI or Fibre channels the disk storage systems to be erased. In addition, the host computer must include a CD-ROM or DVD drive, a USB port, and a minimum of 512K of memory (though 1GB is recommended).

2.2.2.1 Enterprise Disk Storage System Hardware:

FDRERASE/OPEN supports enterprise storage disk subsystems from IBM, EMC and HDS, including the following subsystem models currently available from these vendors:

- IBM DS6000 (1750), DS8000 (2107), ESS (2105) and 3990/9390 subsystems
- EMC Symmetrix DMX, z8000, 8000, and 5000 series subsystems
- Hitachi (HDS) TagmaStore USP (Universal Storage Platform), Lightning 9900V, Freedom 9900, 7700 and 7700E series subsystems.

FDRERASE/OPEN will support all new enterprise storage disk subsystems from the above vendors which are downward compatible with the above models.

2.2.3 Logical Subsystems

The FDRERASE/OPEN solution is composed of three logical subsystems:

- FDRERASE/OPEN application.
- Solaris 10 OS preconfigured to automatically start FDRERASE/OPEN
- "FDRERASE/OPEN key", which unlocks the associated FDRERASE/OPEN application.

[1] Strictly speaking, the TOE is not "installed" in a system, but specific actions occur when the TOE is used for the first time or when it is reinitialized (by wiping the USB flash drive). These actions involve entering a unique, 24-character, "customer key" and changing the authentication password from its default setting.

The FDRERASE/OPEN logical subsystems are shown in the figure below, which also depicts the Physical Components and IT environment.

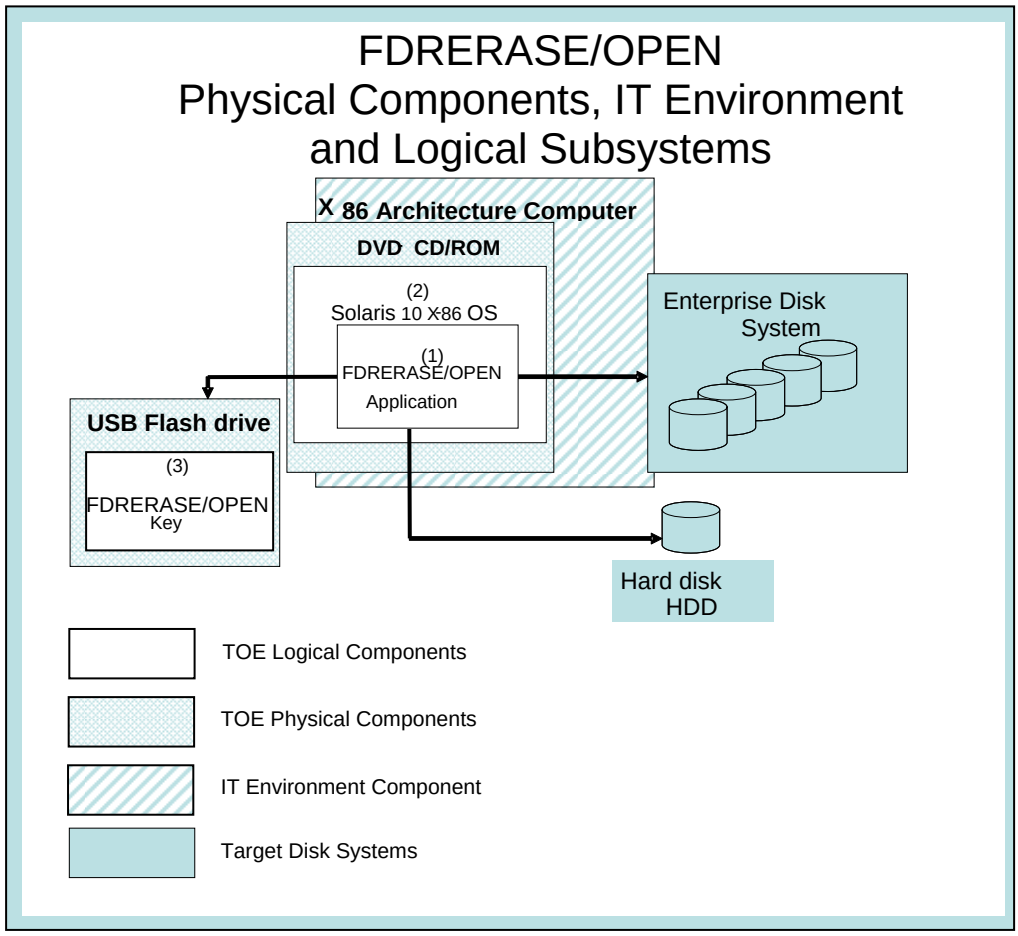

Figure 1: TOE and IT Environment

The FDRERASE/OPEN application and Solaris 10 operating system are provided on a CD-ROM (the "Write Once CD-ROM Compact Disc, aka CD/DVD" depicted in the above figure). FDRERASE/OPEN executes as an interactive process under Solaris 10.

The Solaris 10 operating system (OS) is a Unix-based operating environment developed by Sun Microsystems. Although the core OS has been made into an open source project (OpenSolaris), Solaris 10 proper is still proprietary software. Originally developed to run on Sun's SPARC processors, Solaris now runs on x86 architecture computer systems from other vendors. The Solaris 10 operating system (OS) operating in conjunction with the x86 architecture computer on which it is running does not permit the removal of the FDRERASE/OPEN CD-ROM, while it is running.

The FDRERASE/OPEN key (a USB flash drive as previously stated and depicted in the figure above) serves in the role of a hardware repository that on being initialized acts as a token that allows FDRERASE/OPEN to simplify authenticating the user on subsequent uses of the FDRERASE/OPEN application, as it allows the software to activate without any additional user interactions at start-up. It must be attached to a USB port of the computer that the TOE will operate on prior to booting in order for the TOE to start up successfully. Furthermore, the USB flash drive must remain connected to the USB port throughout the TOE operation. If it is removed, the TOE will complete active security functions and enter an inactive state that does not permit the start of any new functions. Further use of the TOE at this point will require the TOE user to reboot the computer and once again go through the procedure of loading the FDRERASE/OPEN application from the CD-ROM. The procedure of loading the FDRERASE/OPEN application from the CD-ROM will require the USB flash drive (i.e. FDRERASE/OPEN key) associated with the

specific FDRERASE/OPEN application CD-ROM to be attached to a USB port of the computer prior to booting in order for the TOE to start up successfully.

The intended TOE operating environment is an x-86 compatible computer capable of supporting Solaris 10, located in a physically secure environment, and to which is connected by SCSI or Fibre channels the disk storage systems to be erased. In addition, the host computer must include a CD-ROM or DVD drive, a USB port, and a minimum of 512K of memory (though 1GB is recommended).

The TOE performs I/O to the disk controller through the channel programming interface component of Solaris 10. It only overwrites SCSI and Fibre Channel disk volumes that are mounted (on-line) to it and are unmounted (offline) to other systems. However, the TOE will always overwrite Serial ATA (SATA) disk volumes as the SATA interface protocol does not support the command the TOE uses to insure disk volumes are unmounted to other systems.

The TOE issues a command that reserves the disk volume exclusively for its own use. This insures that no other system can mount or access the disk volume during the erasure. If a disk volume is not reserved, it would be possible for that disk volume to be mounted and accessible to another system allowing another user to access the disk volume while the TOE was attempting to overwrite the disk storage. The first check made by the TOE before overwriting a specific disk volume is to see if the disk volume is reserved to it. If the TOE finds it cannot reserve the disk volume exclusively to itself, it reports this to the user and makes no further attempt to overwrite the data on that specific disk volume, except in the case of a SATA disk, which the TOE will always overwrite. Appropriate procedures should be established in the TOE IT environment to ensure SATA disk volumes are unmounted to other systems.

The TOE overwrites every sector on the disk volume in order to erase all data (both user and system data). The TOE writes an increment of sectors. If an I/O operation fails, the I/O will be automatically retried by the disk storage system (hardware) and by standard Solaris 10 software error recovery. If an error is permanent (not recoverable by the hardware or operating system software error recovery routines) or the overwrite operation is canceled by the operator the TOE terminates the process reports the failure by outputting an error status message to the operator, indicating an unsuccessful process, incomplete function or partial overwrite (“FAILED”, “CANCELED”), in the GUI completion bar and records the error or cancellation (i.e., “write failure”, “erase canceled”) with a date and time entry in the log file indicating an unsuccessful process, incomplete function or partial overwrite.

The Solaris 10 OS performs all physical I/O to the SCSI/Fibre/SATA disks and the USB flash drive in response to application program interface requests by the FDRERASE/OPEN application.

2.2.4 Security Functions

This section identifies the security functions that FDRERASE/OPEN provides**.**

2.2.4.1 Security audit

The TOE records the results of its activities associated with disk erasure and verification both in individual disk log files, which are maintained per function per disk (e.g., file “c0t1d0p0.erase.log” is the cumulative log of all erase functions performed on the disk identified as c0t1p0d0), and in a history file that provides a cumulative listing of all TOE activity. Both the individual disk log files and the cumulative history file are stored on the FDRERASE/OPEN key (USB flash drive) associated with the TOE. The TOE GUI provides the capability for the TOE user to view all contents of any of the individual disk log files and the cumulative history file, but does not provide any interfaces for modifying or deleting these files. The TOE user can also view and print the individual disk logs and the cumulative history log that the TOE records on the FDRERASE/OPEN Key from Windows, or any other operating system that will mount a USB flash drive.

Note that normal administrative activity (such as changing passwords) is not audited.

2.2.4.2 User data protection

The TOE provides two disk erasure functions: ERASE and SECUREERASE. Both functions overwrite disk storage to ensure the risk of remaining residual data, if any, is commensurate with the risk of a person scavenging for user data. The ERASE function overwrites a disk volume with one pass (or more, selectable by an input option, up to 8) of binary zero or of hexadecimal bytes chosen by the TOE user. The SECUREERASE function overwrites a disk

volume with a minimum of three passes (or more, selectable by an input option, up to 8) of hexadecimal bytes determined by the TOE.

In addition, the TOE provides the VERIFY function to enable the TOE user to verify that physical sectors of the disk volume have indeed been overwritten sufficiently that no residual information remains.

2.2.4.3 Authentication

The TOE requires the user to authenticate their authority to operate the TOE on initial start-up by entering a "customer key value" and on subsequent start-ups by entering a password prior to allowing the user to access the functions of the TOE. The TOE stores the password, hashed using SHA-1, on the FDRERASE/OPEN key (USB flash drive). The TOE user can lock (prevent) access to the TOE security features at any time. In addition, the TOE will lock the user's session with the TOE if it does not detect any user activity for a user defined number of minutes. In order to unlock the session, the user must re-authenticate their authority by re-entering the password. An authentication password at TOE start-up is a requirement to operate the TOE in a manner that is consistent with CCEVS EAL2 certification prerequisites.

2.2.4.4 Security management

The TOE provides two disk erasure options and identifies the disk storage to be cleared.

The TOE reports to the TOE user the outcome of a disk volume overwrite, including: success; failure to complete because the overwrite function was canceled; failure because the disk volume had already been erased; failure to access the disk because the disk volume could not be reserved to the system; and failure to overwrite a bad disk sector after successive attempts.

The TOE provides the VERIFY function, to enable the user to verify that physical sectors of a disk volume have indeed been overwritten sufficiently that no residual information remains. The TOE reports to the TOE user the outcome of a disk volume verify, including: success; failure to complete because the verify function was canceled; failure because the disk volume had not been erased; and failure to read a bad disk sector after successive attempts.

2.2.4.5 Protection of the TSF

The TOE ensures the security function that is to be executed cannot be bypassed by ensuring (where possible) it has exclusive access to the target disk storage by issuing a hardware command to reserve the disk for its own use before initiating the security function. When a disk volume is reserved, there is no untrusted external interface to the disk storage while the TOE is in operation. To ensure this, the first thing the TOE does during execution for SCSI and Fibre Channel disk is reserve the disk volume. If it fails, the TOE will not attempt to overwrite the disk storage and will report the failure to the TOE user. SATA disk volumes do not support/honor a hardware reserve command. Appropriate procedures should be established in the TOE IT environment to ensure SATA disk volumes are unmounted to other systems.

Throughout the process of performing disk storage overwrite, the TOE continually monitors for any I/O errors on the write and other I/O issued to the disk. Channel hardware and Solaris 10 software error recovery is invoked to recover from errors if possible. If all recovery attempts fail, the user is warned that it was impossible to overwrite the disk. If the hardware will not allow the disk storage to be overwritten, then to absolutely ensure no data is accessible, the failing hard disks may need to be physically removed and destroyed.

3. Security Environment

This section summarizes the threats addressed by the TOE and assumptions about the intended environment of the TOE. Note that while the identified threats are mitigated by the security functions implemented in the TOE (supported as appropriate by security objectives for the non-IT environment), the overall assurance level (EAL 2 augmented with ALC_FLR.2) also serves as an indicator of whether the TOE would be suitable for a given environment.

3.1 Threats

T.Data_remains_after_clear

Any person with programmatic access to the OS can access data on disk storage through programmatic means after the disk storage has been cleared.

T.Data_remnants_remain_after_sanitize

Any person can access data remaining on disk storage after the disk storage has been sanitized, through programmatic means or specialized off-line and off-site attempts to recover data from electro-magnetic remnants of recorded data.

T.Data_scavenging

Any person with physical or programmatic access to disk storage that has been overwritten can exploit predictable overwrite patterns to analytically recover data from it.

T.Errant_overwrite

The TOE user invokes the TOE to overwrite disk storage with an inappropriate erase function, thus leaving the data that was on the disk storage at an unacceptable risk of compromise.

T.Incomplete_overwrite

Unbeknownst to the TOE user, the TOE fails to completely overwrite disk storage, due to write failures, partial overwrites, or the disk storage being on-line and accessible to another program, thus resulting in data remaining on the disk storage when the TOE user believes it is completely erased.

T.Unauthoized_use

An unauthorized user obtains the TOE CD-ROM and its associated key device and uses it to erase disks without appropriate authority.

T.Unattended_TOE

An unauthorized user interferes with the operation of the TOE left unattended by its authorized user, in order to erase disks without appropriate authority, change the TOE to employ an inappropriate erase function or prevent authorized erasure.

3.2 Assumptions

A.Authorized_use

Any person with knowledge of the authentication password and/or the twenty-four character string Customer Key (FDRERASE/OPEN Key) and possession of the FDRERASE/OPEN CD/DVD and the USB flash drive is authorized to install and or use the TOE. Furthermore, an authorized user is authorized to view all information stored on the disk storage systems to be erased.

A.Competent_administration

The persons responsible for administration of the TOE environment and installation of the TOE are trusted, trained, competent, and follow all applicable guidance documentation.

A.Competent_use

The persons responsible for execution of the TOE are trusted, trained, competent, and follow all applicable guidance documentation.

A.Disk_volumes_not accessible

All disks being overwritten are not accessible by any other systems or user programs. That is all the disks honor/support the hardware reserve command or appropriate procedures in the TOE IT environment ensure the disks being overwritten are unmounted to other systems.

A.Secure_environment

The processing resources of the TOE will be located within controlled access facilities that will prevent unauthorized physical access. Furthermore, the underlying hardware environment operates correctly and is configured to support the operation of the TOE.

A.Proper_procedures

TOE users will abide by all higher authority directives, which could include a second person use of the TOE to verify the person executing the TOE overwrite operation did so on the intended disks, employing appropriate overwrite options.

A.Reliable_clock

The TOE operating environment includes a reliably functioning clock and issues a warning if there is no reliably functioning clock or the clock fails.

4. Security Objectives

This section summarizes the security objectives for the TOE and its environment.

4.1 Security Objectives for the TOE

O.Authenticated_use

The TOE shall require a user to authenticate to the TOE prior to allowing the user to interact with the TOE and shall allow authenticated users to lock the TOE preventing unauthenticated users access to the TOE security functions. Furthermore, the TOE shall lock the user's interactive session if it does not detect any user activity for a user specified number of minutes, and shall require authentication in order to unlock the user session.

O.Erase_clears

The TOE shall provide a capability to erase all data on disk storage so as to make the data inaccessible to an operating system user running a non-authorized or authorized program attempting to read the original data, running anywhere that has access to the disk storage.

O.Record_of_operation

The TOE shall provide to the user a record of its operation for each overwrite function. Upon completion of an overwrite function, the TOE shall provide a record of the overwrite function used, the disks overwritten and the status of the overwrite results for each disk volume overwritten. The record will indicate if the overwrite was successful or unsuccessful. Furthermore, the TOE shall report to the user, during the progress of an overwrite function, the following occurrences that indicate the overwrite may not be successful: write failures to the disk; other I/O failures to the disk; cancellation of the security function.

O.Secure_erase_sanitizes

The TOE shall provide a capability to securely erase all data on a disk so as to make the data inaccessible: to an operating system user running a non-authorized or authorized program attempting to read the original data, running anywhere that has access to the disk; through the use of off-line special tools designed to perform data recovery or by sophisticated laboratory techniques applied to hard drives removed from the control unit.

O.Verified_operation

When the TSF has completed an erase function, there is significant assurance that the erase function has performed appropriately and overwritten every sector on the disk storage. The TOE shall provide a capability to verify that disk storage has been properly erased.

4.2 Security Objectives for the IT Environment

OE.Reliable_clock

The IT environment will provide a reliably functioning clock and will issue a warning if there is no reliably functioning clock or the clock fails.

4.3 Security Objectives for the Environment

OE.Authorized_use

Those responsible for the TOE and its use within the intended environment will ensure only persons authorized to use the TOE will have knowledge of the authentication password and/or the twenty-four character string Customer Key (FDRERASE/OPEN Key) and possession of the FDRERASE/OPEN CD/DVD and the USB flash drive. Furthermore, those responsible for the TOE and its use within the intended environment will ensure an authorized user is authorized to view all information stored on the disk storage systems to be erased.

OE.Competent_staff

Those responsible for the TOE will ensure the administrative staff of the TOE environment and the users of the TOE are trusted, trained, competent, and follow all applicable guidance documentation.

OE.Controlled_facility

Those responsible for the TOE will ensure physical access to the TOE and its operational environment is controlled so that unauthorized physical access to the TOE is prevented.

OE.Operational_procedures

Those responsible for the TOE will ensure the capabilities of the TOE will be utilized in accordance with any higher authority directives or operational 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.

5.1 TOE Security Functional Requirements

The following table identifies the SFRs that are satisfied by the TOE. The minimum strength of function level for the TOE SFRs is SOF-basic. An explicit strength of function claim is appropriate for FIA_UAU.2, and this is also SOF-basic. The rationale for these claims is provided in Section 8.4 of this ST.

Requirement Class	Requirement Component
FAU: Security audit	FAU_GEN.1: Audit data generation
	FAU_SAR.1: Audit review
	FAU_STG.1: Protected audit trail storage
FCS: Cryptographic support	FCS_COP.1: Cryptographic operation
FDP: User data protection	FDP_BDE_EXP.1: Basic disk erasure
	FDP_SDE_EXP.1: Secure disk erasure
	FDP_DEV_EXP.1: Disk erasure verification
FIA: Identification and authentication	FIA_UAU.2: User authentication before any action
	FIA_UAU.6: Re-authenticating
FMT: Security management	FMT_SMF.1: Specification of Management Functions
FPT: Protection of the TSF	FPT_RVM.1: Non-bypassability of the TSP
	FPT_SEP.1: TSF domain separation
FTA: TOE access	FTA_SSL.1: TSF-initiated session locking
	FTA_SSL.2: User-initiated locking

Table 1: TOE Security Functional Requirements

5.1.1 Security audit (FAU)

5.1.1.1 Audit data generation (FAU_GEN.1)

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) ~~Start-up and shutdown of the audit functions~~;

b) All auditable events for the **[*not specified*]** level of audit; and

c) **[execution of ERASE, SECURE ERASE and VERIFY function]**.

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, ~~subject identity,~~ and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, **[**

- **for ERASE: disk identification, number of passes, overwrite pattern, write failures, partial overwrites;**
- **for SECURE ERASE: disk identification, number of passes, write failures, partial overwrites;**
- **for VERIFY: disk identification, read failures]**.

Application Note: *The TSF does not provide a capability to startup or shutdown the audit function. Auditing is always enabled. Therefore, FAU_GEN.1.1 has been refined to accurately specify TSF' auditable events.*

Application Note: *The TSF is the only subject within the TSC, and so recording the subject identity adds no value to the content of the audit record. Therefore, FAU_GEN.1.2 has been refined to accurately specify the minimum information recorded within each audit record.*

Application Note: *There is no message output that explicitly says 'partial overwrite"… a message recording "Cancel" or "Failure" is the indication that an over write did not complete… any erase operation that starts but does not complete is a "partial overwrite" rather than a complete overwrite of the intended disk.*

5.1.1.2 Audit review (FAU_SAR.1)

FAU_SAR.1.1 The TSF shall provide **[the TOE user]** with the capability to read **[all audit information]** from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

Application Note: *The TSF records all audit information in Log Files, i.e. individual cumulative logs for each TOE security function performed on the individual disks, and in a History File, i.e. a cumulative accounting of all TOE activity since the initialization of the USB flash drive for this installation of the TOE.*

5.1.1.3 Protected audit trail storage (FAU_STG.1)

FAU_STG.1.1 The TSF shall protect the stored audit records from unauthorised deletion.

FAU_STG.1.2 The TSF shall be able to **[*prevent*]** unauthorised modifications to the stored audit records in the audit trail.

5.1.2 Cryptographic support (FCS)

5.1.2.1 Cryptographic operation (FCS_COP.1)

FCS_COP.1.1 The TSF shall perform **[cryptographic hashing]** in accordance with a specified cryptographic algorithm **[SHA-1]** and cryptographic key sizes **[160 bits]** that meet the following: **[FIPS PUB 180-2]**.

5.1.3 User data protection (FDP)

5.1.3.1 Basic disk erasure (FDP_BDE_EXP.1)

FDP_BDE_EXP.1.1 The TSF shall be able to overwrite selected disk volumes:

a) up to a maximum eight overwrite passes, as specified by the user, with a data pattern for each pass, selected by the user, comprising:

- two hexadecimal characters specified by the user; or
- a TSF-generated random pattern;

b) a minimum of one overwrite pass with binary zeroes, by default.

5.1.3.2 Secure disk erasure (FDP_SDE_EXP.1)

FDP_SDE_EXP.1.1 The TSF shall be able to overwrite selected disk volumes with a random data pattern determined by the TSF, followed by its complement, followed by another random pattern determined by the TSF (i.e. the minimum three overwrite passes):

a) up to a maximum eight overwrite passes, as specified by the user;

b) a minimum of three overwrite passes, by default.

5.1.3.3 Disk erasure verification (FDP_DEV_EXP.1)

FDP_DEV_EXP.1.1 The TSF shall provide the capability to verify that a disk has been erased.

5.1.4 Identification and authentication (FIA)

5.1.4.1 User authentication before any action (FIA_UAU.2)

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

5.1.4.2 Re-authenticating (FIA_UAU.6)

FIA_UAU.6.1 The TSF shall re-authenticate the user under the conditions **[changing password, unlocking an interactive session]**.

5.1.5 Security management (FMT)

5.1.5.1 Specification of Management Functions (FMT_SMF.1)

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

- **allow selection of an appropriate overwrite option;**
- **verification that the data on the disk storage has been successfully overwritten]**.

5.1.6 Protection of the TSF (FPT)

5.1.6.1 Non-bypassability of the TSP (FPT_RVM.1)

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

5.1.6.2 TSF domain separation (FPT_SEP.1)

FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

5.1.7 TOE access (FTA)

5.1.7.1 TSF-initiated session locking (FTA_SSL.1)

FTA_SSL.1.1 The TSF shall lock an interactive session after **[a TOE user specified number of minutes]** by:

a) clearing or overwriting display devices, making the current contents unreadable;

b) disabling any activity of the user's data access/display devices other than unlocking the session.

Application Note: *TSF session locking prevents alteration of any active functions or activation of any inactive functions by disabling a user's ability to select any of the functions on the icon line except for EXIT. Operations that are in process when access to a session locks continue to conclusion, operations that were selected and are waiting to process, when access to a session locks, will activate when the resources they are waiting on become available even though the access to the session remains locked. Any attempt to employ the user interface results in a password prompt.*

If the 'Hide window when prompting for password" option on the Password Setting dialog screen is selected, any attempt to employ the user interface in a locked session results in a password

prompt and causes the TOE Window to become invisible. The TOE Window then remains invisible until a valid password is entered. This setting, i.e. to clear the screen is a requirement to operate the TOE in a manner that is consistent with CCEVS EAL2 certification prerequisites.

FTA_SSL.1.2 The TSF shall require the following events to occur prior to unlocking the session: **[user authentication]**.

5.1.7.2 User-initiated locking (FTA_SSL.2)

FTA_SSL.2.1 The TSF shall allow user-initiated locking of the user's own interactive session, by:
a) clearing or overwriting display devices, making the current contents unreadable;
b) disabling any activity of the user's data access/display devices other than unlocking the session.

FTA_SSL.2.2 The TSF shall require the following events to occur prior to unlocking the session: **[user authentication]**.

5.2 IT Environment Security Functional Requirements

The following table identifies the SFR that is assumed to be provided in the environment of the TOE.

Requirement Class	Requirement Component
FPT: Protection of the TSF	FPT_STM.1: Reliable time stamps

Table 2: IT Environment Security Functional Requirements

5.2.1 Protection of the TSF (FPT)

5.2.1.1 Reliable time stamps (FPT_STM.1)

FPT_STM.1.1 The ~~TSF~~ **IT Environment** shall be able to provide reliable time stamps for its own **and TOE** use.

5.3 TOE Security Assurance Requirements

The security assurance requirements for the TOE are the EAL 2 augmented with ALC_FLR.2 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.2: Configuration items
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.1: Descriptive 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_FLR.2: Flaw reporting procedures
ATE: Tests	ATE_COV.1: Evidence of coverage
	ATE_FUN.1: Functional testing
	ATE_IND.2: Independent testing - sample
AVA: Vulnerability assessment	AVA_SOF.1: Strength of TOE security function evaluation
	AVA_VLA.1: Developer vulnerability analysis

Table 3: EAL 2 augmented with ALC_FLR.2 Assurance Requirements

5.3.1 Configuration management (ACM)

5.3.1.1 Configuration items (ACM_CAP.2)

ACM_CAP.2.1d The developer shall provide a reference for the TOE.
ACM_CAP.2.2d The developer shall use a CM system.
ACM_CAP.2.3d The developer shall provide CM documentation.
ACM_CAP.2.1c The reference for the TOE shall be unique to each version of the TOE.
ACM_CAP.2.2c The TOE shall be labeled with its reference.
ACM_CAP.2.3c The CM documentation shall include a configuration list.
ACM_CAP.2.4c The configuration list shall uniquely identify all configuration items that comprise the TOE.
ACM_CAP.2.5c The configuration list shall describe the configuration items that comprise the TOE.
ACM_CAP.2.6c The CM documentation shall describe the method used to uniquely identify the configuration items that comprise the TOE.
ACM_CAP.2.7c The CM system shall uniquely identify all configuration items that comprise the TOE.
ACM_CAP.2.1e 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 Descriptive high-level design (ADV_HLD.1)

ADV_HLD.1.1d The developer shall provide the high-level design of the TSF.
ADV_HLD.1.1c The presentation of the high-level design shall be informal.
ADV_HLD.1.2c The high-level design shall be internally consistent.
ADV_HLD.1.3c The high-level design shall describe the structure of the TSF in terms of subsystems.
ADV_HLD.1.4c The high-level design shall describe the security functionality provided by each subsystem of the TSF.
ADV_HLD.1.5c 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.1.6c The high-level design shall identify all interfaces to the subsystems of the TSF.
ADV_HLD.1.7c The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.
ADV_HLD.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADV_HLD.1.2e 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 behavior 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 behavior 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 Flaw reporting procedures (ALC_FLR.2)

ALC_FLR.2.1d The developer shall provide flaw remediation procedures addressed to TOE developers.
ALC_FLR.2.2d The developer shall establish a procedure for accepting and acting upon all reports of security flaws and requests for corrections to those flaws.
ALC_FLR.2.3d The developer shall provide flaw remediation guidance addressed to TOE users.
ALC_FLR.2.1c The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.
ALC_FLR.2.2c 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.2.3c The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.
ALC_FLR.2.4c 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.2.5c The flaw remediation procedures documentation shall describe a means by which the developer receives from TOE users reports and enquiries of suspected security flaws in the TOE.
ALC_FLR.2.6c The procedures for processing reported security flaws shall ensure that any reported flaws are corrected and the correction issued to TOE users.
ALC_FLR.2.7c The procedures for processing reported security flaws shall provide safeguards that any corrections to these security flaws do not introduce any new flaws.
ALC_FLR.2.8c The flaw remediation guidance shall describe a means by which TOE users report to the developer any suspected security flaws in the TOE.
ALC_FLR.2.1e 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 Evidence of coverage (ATE_COV.1)

ATE_COV.1.1d The developer shall provide evidence of the test coverage.
ATE_COV.1.1c The evidence of the test coverage shall show the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.
ATE_COV.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.6.2 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.

5.3.6.3 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 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.

5.3.7.2 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

6.1.1 Security audit

The TOE generates audit records for Disk Log Files, i.e. individual cumulative logs for each TOE security function performed on the individual disks, and for a History File, i.e. a cumulative accounting of all TOE activity since the initialization of the USB flash drive as the FDRERASE/OPEN Key for this installation. Audit records contain detailed information for the following auditable events:

- execution of the ERASE function
- execution of the SECURE ERASE function
- execution of the VERIFY function.

Audit records written to a Disk Log File include, at minimum, the following for each auditable event:

- Start and Finish time of each security function performed on the device
- Disk identification (identifier of an individual disk, which is also included in the log file name)
- Type of event (i.e., ERASE, SECURE ERASE, or VERIFY)
    - the number of passes performed (for an ERASE or SECURE ERASE function)
    - the chosen overwrite pattern (for an ERASE function – for SECURE ERASE, the overwrite pattern is randomly generated by the TSF and cannot be chosen by the user)
- Event outcome (success or failure)
- Any associated error messages.

Audit records written to the History File include, at minimum, the following for each auditable event:

- Date and time that event commenced and concluded.
- Type of event (i.e., ERASE, SECURE ERASE, or VERIFY)
- Disk identification (identify of an individual disk)
- Event outcome (success or failure).

Audit records will include, as appropriate for the ERASE and SECURE ERASE functions, occurrences of any write failures or cancellations, which would indicate that an erase operation did not complete. The audit records will include, as appropriate for the VERIFY function, any read failures or cancellations. If an I/O failure occurs during a disk write or read operation due to disk surface failures, the TSF makes a series of attempts to retry the overwrite or read of the bad disk sector(s); if this is unsuccessful (i.e. it is a permanent unrecoverable error), the TSF reports the error to the GUI, creates an audit record entry for the failure and terminates the security function. An ERASE and a SECURE ERASE function will as a result conclude with only a partial overwrite of the disk.

The TSF writes audit records to a single cumulative History File, on the USB flash drive FDRERASE/OPEN Key, identified as “fdrerase.log” and to multiple Disk Log Files, identified as “*disk*.*function*.log”, where “*disk*” is the unique identifier for each disk known to the TSF and “*function*” is the security function (ERASE, SERCURE ERASE or VERIFY) that individual cumulative log file is maintaining a history of for the specific disk.

The TOE GUI provides the capability for the TOE user to view the contents of any of the individual Disk Log Files and the cumulative History File. The TSF writes audit records in a format suitable for a TOE user to view and print the individual Disk Log Files that the TOE records on the FDRERASE/OPEN Key USB flash drive, from Windows, or any other operating system that will mount a USB flash drive. The TOE writes the contents of the History File initially in a compressed format to a file named "fdrerase.history" that is readable by the user only by using the interface provided by the TOE, which generates the "fdrerase.log" file. Unlike the individual Data Log Files, the contents of "fdrerase.history" are not readily interpretable when viewed using a text editor or similar utility on Windows or any other operating system capable of mounting a USB flash drive.

The TOE GUI does not provide any capability to modify or delete the individual Disk Log Files and the cumulative History File that the TOE records on the FDRERASE/OPEN Key USB flash drive. However, notice should be taken that there is no protection against access, modification or deletion if the FDRERASE/OPEN Key USB flash drive is accessed on Windows, or any other operating system that will mount a USB flash drive. Protection preventing access to or modification of the information recorded on the FDRERASE/OPEN Key USB flash drive is only provided when the USB is used in conjunction with the TOE.

Warning: The audit data logged for each security function operation is minimal and a user could record the output from thousands, if not tens of thousands, of erases, verifies, etc. on a 1/2 GB stick. However a USB can provide only a finite amount of memory. Misuse of the PRINT function in particular could fill just about any size memory stick. In the event a user exhausts the available memory on the memory stick, the FDRERASE/OPEN User Interface continues to operate but any new functions requiring space on the stick would fail when starting. Nothing is overwritten, the GUI displays the word failed in a red highlighted text in the "% Complete" column and if possible FDRERASE/OPEN records the message "No space left on device, "*name of requested function*" failed" in the device log file. The User Manual describes procedures for dealing with this circumstance.

The Security audit function is designed to satisfy the following security functional requirement:

- FAU_GEN.1: As indicated above, the TSF generates records for the execution of the ERASE, SECURE ERASE, and VERIFY functions, identifying the target disk, including the date and time the function executed, its outcome, and information relevant to any occurrences of write errors, partial overwrites, and read failures. Since the TSF automatically generates all audit records and this capability cannot be turned off, the requirement to audit start-up and shutdown of the audit functions is vacuously satisfied.
- FAU_SAR.1: The TOE GUI provides the TOE user with the capability of viewing and interpreting the contents of all individual Disk Log Files and the cumulative History File stored on the FDRERASE/OPEN Key USB flash drive. The TOE user can also view and print the individual Disk Log Files that the TOE records on the FDRERASE/OPEN Key USB flash drive from Windows, or any other operating system that will mount a USB flash drive.
- FAU_STG.1: The TOE does not provide any interfaces that permit the TOE user to modify or delete the log files stored on the FDRERASE/OPEN Key USB flash drive. While the FDRERASE/OPEN Key USB flash drive remains connected to the computer on which the TOE is operating, the only interface presented to the user is the TOE GUI, which provides commands for viewing the log files, but not for modifying or deleting them. Furthermore, the TOE does not provide access to an operating system level command line that might otherwise allow direct access to the FDRERASE/OPEN Key USB flash drive. Note that the TOE cannot provide this protection when it is not operating or when the FDRERASE/OPEN Key USB flash drive has been removed and connected to a computer running Windows, or any other operating system that will mount a USB flash drive.

6.1.2 User data protection

The TOE can be instructed through its GUI to perform either an ERASE or a SECURE ERASE on one or more specified disk volumes. Both ERASE and SECURE ERASE overwrite (i.e., erase) all data on the specified disk storage with a hexadecimal pattern. The two commands provide different default behaviors and different options for selecting overwrite patterns. After an ERASE, no residual information remains that can be accessed programmatically in the TOE's intended environment. After a SECURE ERASE, no residual information remains that can be accessed either programmatically or through the use of specialized techniques.

When the ERASE function is selected, the TOE user has an option to select the pattern used to overwrite disk sectors. The pattern is specified as a hexadecimal byte (i.e., two hexadecimal characters), used to overwrite all locations on the disk. The TOE user can optionally specify a different data pattern (i.e., a different hexadecimal byte) to be used on each overwrite pass. If the ERASE random pattern option is selected (by entering hexadecimal byte 'FE' as the overwrite pattern), the TOE will generate random hexadecimal bytes using an internal proprietary algorithm and overwrite all data on the disk storage with random hexadecimal bytes in the same manner as described below for SECURE ERASE. The TOE user can select to have the ERASE function make from 1 to 8 overwrite passes on a disk.

When the SECURE ERASE function is selected, the TSF selects a random hexadecimal byte for the first pass followed by the ones complement of the byte from the first pass to reverse all bits in a hexadecimal byte. A third overwrite is performed with a new random hexadecimal byte. More than 3 overwrites can be selected to meet other requirements; the fourth pattern will be the one's complement of the third pattern. The fifth overwrite pass pattern is randomly generated, the sixth pattern will be the complement of the fifth pattern, the seventh pattern will be a new random pattern and the eight will be its complement.

The TOE can also be instructed through its GUI to perform a VERIFY function. The VERIFY function attempts to read selected areas of a specified disk volume to verify that all data previously written on the disk storage has actually been overwritten. The TOE user can also specify that the VERIFY function read every sector on the specified disk volume.

The User data protection function is designed to satisfy the following security functional requirements:

- FDP_BDE_EXP.1: The ERASE function overwrites all data on specified disk storage. By default, it overwrites every sector on selected disks once using a pattern of binary zeroes (hexadecimal '00'). However, the user has the option of specifying multiple overwrites, up to 8, and of specifying the overwrite pattern for each overwrite pass.
- FDP_SDE_EXP.1: The SECURE ERASE function overwrites all data on specified disk storage. By default, it overwrites every sector on selected disks three times, as follows: the first overwrite uses a random data pattern; the second overwrite uses the complement of the random data pattern used in the first overwrite; and the third overwrite uses a new random pattern. Additionally, the user has the option of specifying that more than three overwrites are performed, up to a maximum of 8. When more than three overwrites are specified, the fourth overwrite uses the complement of the pattern in the third overwrite, the fifth and sixth overwrite are with a new random pattern and its complement, and the seventh and eighth overwrite use another new random pattern and its complement.
- FDP_DEV_EXP.1: The VERIFY function can be selected by the TOE user to verify that all sectors on specified disk storage have been overwritten by the ERASE or SECURE ERASE function, thereby verifying that any previous information content is no longer available.

6.1.3 Authentication

The TOE not the operating system enforces password authentication. The TOE requires the user to enter a password in response to a GUI authentication message prior to allowing the user to access any of the other functions of the TOE. When the TOE is first installed and started up (i.e. activated and configured), the default password is "fdrerase", but this must be changed immediately as it cannot be reused, unless the TOE is unconfigured and reactivated. The new password must be at least 8 characters long and include at least one member from at least three of the following four sets of characters: upper case alphabetic (i.e., A..Z); lower case alphabetic (i.e., a..z); numeric (i.e., 0..9); and "specials" (i.e., the printable non-alphanumeric characters on a standard keyboard, such as ~!@#$%^&*()_+, etc.). The TSF hashes the new password, using the SHA-1 hash algorithm provided by the Solaris 10 OS, and stores it on the FDRERASE/OPEN Key USB flash drive.

The TOE provides the capability for the user to change the password at any time, but the user must authenticate this action by entering the current password in order for the new password to be accepted (including when changing the password the very first time).

The TOE user can lock the interactive session at any time, preventing access to the TOE security features and overwriting the screen with an authentication request message that requires a password response. TSF session locking prevents alteration of any active functions or activation of any inactive functions by disabling a user's ability

to select any of the functions on the icon line except for EXIT. Just moving the mouse to scroll what is already on the screen or hitting the keyboard e.g. space bar, is not considered an attempt to employ the user interface. Any attempt to employ the user interface however results in a password prompt. The session locking option 'Hide window when prompting for password" on the TOE Password Setting dialog screen when selected causes the TOE Window to become invisible when a password prompt appears. This setting, i.e. to clear the screen, is a requirement to operate the TOE in a manner that is consistent with CCEVS EAL2 certification prerequisites.

Additionally, the TOE monitors the GUI for user activity[2]. If the TOE does not detect any user activity for a number of minutes as specified by the user, it locks the interactive session. The user must re-authenticate to the TOE (by entering the correct password as described above) in order to unlock the session and continue interaction with the TOE.

An authentication password can not be reset unless the user is in possession of the current authentication password and is not recoverable if forgotten. Consequently care should be taken to prevent the loss of the password as if that occurs the only way to use the TOE is to clear all the information from the FDRERASE/OPEN Key USB flash drive and reinitialize the TOE with a valid 'customer key". INNOVATION can provide a replacement 'customer key'.

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

- FIA_UAU.2: The TOE requires the user to enter the correct password in order to complete initialization and allow the user to access TOE functionality.
- FIA_UAU.6: The TOE requires the user to enter the correct password in order to change the password to a new value, and to unlock the interactive session.
- FTA_SSL.1: The TOE locks the user's interactive session if there is no user activity detected for a number of minutes as specified by the user. The user must re-authenticate by entering the correct password in order to unlock the interactive session and resume interaction with the TOE.
- FTA_SSL.2. The TSF allows the user to initiate locking of the user's own interactive session, overwriting the GUI display with an authentication request message to make the current contents unreadable and disabling any use of the data access/display devices other than unlocking the session. The user must re-authenticate by entering the correct password in order to unlock the interactive session and resume interaction with the TOE.
- FCS_COP.1: The TOE hashes the user password using the SHA-1 cryptographic hashing algorithm as specified in FIPS PUB 180-2 Secure Hash Standard, 1 August 2002. The SHA-1 algorithm produces a 160-bit long hash of the password.

6.1.4 Security management

The TOE provides two overwrite operation functions and identifies the disk storage to be cleared. If the ERASE function is selected, the TOE user can select the number of passes to be performed (1 to 8) and may: choose to allow the TOE to overwrite with binary zeros; specify the overwrite pattern for particular passes; or direct the TSF to generate a random pattern for particular passes. The TSF enforces random patterns and their complements for the SECURE ERASE function (minimum of 3 passes), but allows the user to specify if more than 3 passes (up to a maximum of 8) are to be performed.

The TOE provides the VERIFY function to determine that an overwrite function completed. The VERIFY attempts to read selected areas of the disk storage to verify that all data previously on the disk storage has actually been overwritten.

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

[2] Defined as interaction with the GUI, such as selecting and initiating some function. Just moving the mouse to scroll what is on the screen or hitting the space bar is not considered 'user activity'.

- FMT_SMF.1: The TSF provides the capability for the user to select the overwrite function appropriate to the user's requirements and specify options to direct the operation of the overwrite function. The TSF also provides the capability for the user to verify that an overwrite function completed successfully.

6.1.5 Protection of the TSF

FDRERASE/OPEN is an application written in the C and JAVA programming languages. It is loaded onto a computer from a CD-ROM compact disc by a person authorized to possess that CD-ROM and an associated key device (USB flash drive). The CD-ROM containing FDRERASE/OPEN also contains a copy of the Sun Solaris 10 operating system, preconfigured to automatically start FDRERASE/OPEN after the boot of Solaris 10 is complete. This method results in Solaris 10 invoking FDRERASE/OPEN as the sole user application executing on the computer. The "FDRERASE/OPEN key" concept is that a specific USB stick can be tied to a specific CD/DVD using the unique manufacture's serial number recorded on the USB stick and recording that USB serial number on the CD/DVD during the FDRERASE/OPEN creation process. The USB flash drive contains validation codes which match the CD-ROM. These codes are compared at startup. If they do not match, the TOE will exit. The USB flash drive is also used to store options, logs, and history records.

The TSF ensures that only disk storage that has been placed off-line (unmounted) to other systems is available to the TSF before it allows the TOE user to continue with the ERASE and SECURE ERASE functions. Since the disk storage must be off-line, there is no untrusted external interface to the disk storage while the TOE is in operation. To ensure this, the first thing the TSF does during execution is reserve the disk volume. If it can not, the TSF will not attempt to overwrite the disk storage and will report the failure to the user. It should be noted, however, that SATA disk volumes provide a special case, since the SATA interface protocol does not support the command the TOE uses to reserve disk volumes to itself. The TSF will always overwrite SATA disk volumes, and so it is an assumption of use that the TOE user will take necessary steps to ensure the computer hosting the TOE is the only computer able to communicate with target SATA disk volumes prior to invoking the TOE.

Throughout the process of performing a disk storage overwrite, the TSF continually monitors for any I/O errors on the write, loss of exclusive access and other I/O issued to the disk. X86 architecture computer system channel hardware and Solaris OS software error recovery is invoked to recover from errors if possible. When I/O commands are issued, I/O errors will indicate if some data could not be written to the disk storage. If all hardware and operating system software recovery attempts fail on any IO (i.e. a permanent error), it is reported to the TOE user (via an interactive GUI) and logged. The TOE user is warned that user data may still reside on the damaged disk, but that it was impossible to write to an area of the disk storage. If the hardware will not allow a portion of the disk storage to be overwritten, then to absolutely ensure no data is accessible, the failing hard disks may need to be physically removed and destroyed.

During operation of either the ERASE or the SECURE ERASE function on a specified disk volume, if a single write error is encountered, or there is a loss of exclusive control the TSF sends a message to the TOE user identifying the disk volume, and that the overwrite was a failure. The TSF then terminates the overwrite of that disk volume.

The Protection of the TSF function is designed to satisfy the following security functional requirements:

- FPT_RVM.1: The TSF is invoked via a GUI (graphic user interface) command selection specifying the security function to be executed (ERASE, SECURE ERASE or VERIFY) and its parameters. There is no other interface to the TSF. The TSF ensures the ERASE and SECURE ERASE functions cannot be bypassed by ensuring (where possible) it has exclusive access to the target disk storage. If the TSF determines that exclusive access cannot be guaranteed, it terminates with an appropriate message to the TOE user that the overwrite operation did not complete.
- FPT_SEP.1: The TOE is architected such that when the Solaris 10 OS initially boots from the CD-ROM, the FDRERASE/OPEN application is the only user application running on the computer. In addition, the TOE operates only if the FDRERASE/OPEN Key (USB flash drive) associated with the CD-ROM via the unique validation code is attached to the host computer. This ensures the correct components of the TOE are always present and cannot be substituted.

6.2 TOE Security Assurance Measures

6.2.1 Configuration management

The configuration management measures applied by Innovation ensure that configuration items are uniquely identified, and that documented procedures are used to control and track changes that are made to the TOE. Innovation performs configuration management on the following configuration items:

- TOE code,
- Design information,
- Test documentation,
- User guidance (no administrator role that is separate),
- Delivery and operation information,
- Vulnerability analysis documentation,
- Flaw remediation information (bug tracking),
- Security policy model information,
- and the CM documentation.

Furthermore Innovation performs configuration management of all TSF tests.

These activities are documented in the following Configuration Management (ACM_CAP.2) Configuration Items submission:

- EROCFM10 – The Innovation Data Processing Open System Software Development Configuration Management Developer Guide

This document identifies Innovation Data Processing uses a Version Control System (VCS) and an Access Control Mechanism (ACM) to manage change tracking and code protection:

A Version Control System (VCS) is used to manage a central *repository* of product related files.

The product repository is organized as a tree of directories and files. The hierarchy of the repository directory branches represent:

- TEST Level (Development Project Repository Trunk containing versions of files tagged for identification)
- BETA Level (directory branches containing versions shipped to customers willing to test pre-GA versions)
- GA Level (directory branches containing versions shipped to customers as production versions)
    - Directory branches correspond to production “Version” releases (e.g., V02xx)
        - Tagged versions in a directory branch correspond to a “Version” and “Level” number, (e.g., V0201)

Developers have their own individual local copy of the Project Repository Trunk into which the can copy (check out), update and then return (commit) versions of project files. Individual levels of the repository directory branch hierarchy contain files relating to:

- SOURCE (human readable text statements used to generate executable files)
    - GUI (Graphic User Interface)
        - JAVA
        - Native C (HEADERS, MESSAGES, PANELS, SKELETON)
    - Utilities (Configurations and Reporting)

  - Native C (HEADERS, MESSAGES, PANELS, SKELETON)
- MAINT (description of maintenance applied to or created for a specific maintenance version)
- TESTS (scripts used to verify the version)

An Access Control Mechanism (ACM) is used to limit access to the repository

The Configuration management assurance measure satisfies the following assurance requirement:

- ACM_CAP.2.

6.2.2 Delivery and operation

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

As part of the process of generating the TOE in preparation for delivery to a customer, a unique <24> character string <Customer Key> is also generated. This string is provided to the customer separately from the TOE deliverable itself, recorded on the associated FDRERASE/OPEN CD/DVD and must be entered by the customer when the TOE is initially installed in order to activate and configure the TOE. If the FDRERASE/OPEN Key USB flash drive is erased the TOE is effectively unconfigured and must be reactivated before it can be used again.

This configuration/activation mechanism is entirely separate and distinct from the session password mechanism used in the Authentication security function.

These activities are documented in the following Delivery and Operation (ADO_DEL.1) and Delivery, Installation, Generation and Start-up (ADO_IGS.1) submission:

- ERODOP10 – INNOVATION Data Processing Open System Software Distribution Process Description and Open System Software Distribution Facility User Guide

The Delivery and operation assurance measure satisfies the following assurance requirements:

- ADO_DEL.1
- ADO_IGS.1.

6.2.3 Development

Innovation has documents describing all facets of the design of the TOE. The TSF and its external interfaces are described. The description includes the purpose and method of use of all of the TSF interfaces, and all of the security functions are completely described.

These documents describe all the TOE interfaces (both external and between components), the high level design of the TOE (in terms of components), and correspondence between the available design abstractions (including the ST).

The TOE design is documented in the following Development Activity, Functional Specification, High-Level Design, and Representation Correspondence (ADV_FSP.1, ADV-HLD.1 and ADV_RCR.1) submission:

- ERODES14 – FDRERASE/OPEN Solution Functional Specification, High-Level Design and Representation Correspondence Document

The Development assurance measure satisfies the following assurance requirements:

- ADV_FSP.1

- ADV_HLD.1
- ADV_RCR.1.

6.2.4 Guidance documents

Innovation 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. The guidance describes the administrative functions and interfaces available to TOE administrators, any assumptions regarding user behavior that are relevant to the secure operation of the TOE, and all security parameters (including secure values as appropriate) that are under the control of the administrator.

The administrator and user guidance is provided in the following Guidance Documents (AGD_ADM.1) and Administrator and User Guidance (AGD_USR.1) submission:

- ERODOC10 – FDRERASE/OPEN User Manual and Installation Guide

The Guidance documents assurance measure satisfies the following assurance requirements:

- AGD_ADM.1
- AGD_USR.1.

6.2.5 Life cycle support

Innovation employs a process where security flaws discovered by customers and Innovation are tracked and corrected by the developer. Innovation bug reconciliation process provides assurance that the TOE is maintained and flaws are corrected in the TOE, first by maintenance releases of the programs and later by new production releases.

Innovation describes the method used to provide flaw information, correction and guidance on corrective actions to TOE users in the following Life Cycle Support and Flaw Remediation (ALC_FLR.2) submission:

- EROBUG10 – Innovation Data Processing Software Product Life Cycle Maintenance Support (Bug Track) User Guide

The Life cycle support assurance measure satisfies the following assurance requirement:

- ALC_FLR.2.

6.2.6 Tests

The test documents describe the overall test plan, testing procedures, the tests themselves, including expected and actual results. In addition, these documents describe how the functional specification has been appropriately tested.

These activities are documented in the following Test Activity, Coverage, Functional and Independent Testing (ATE_COV.1, ATE_FUN.1 and ATE_IND.2) submission:

- EROATE12 – FDRERASE/OPEN Solution Testing Procedures and Test Documentation

The Tests assurance measure satisfies the following assurance requirements:

- ATE_COV.1
- ATE_FUN.1
- ATE_IND.2 – to be accomplished by the evaluation team.

6.2.7 Vulnerability assessment

Innovation has conducted strength of function analysis to identify and analyze permutational or probabilistic security mechanisms implemented in the TOE. The ST specifies the use of a password mechanism to support the Authentication security function, and the SOF analysis demonstrates that this mechanism meets at least SOF-basic.

Innovation performs regular vulnerability analyses of the entire TOE (including documentation) to identify weaknesses that can be exploited in the TOE. Innovation's Vulnerability analysis describes the obvious vulnerabilities identified in the TOE, the operating system, and the various disk storage manufactures on which the TSF operate. Each candidate vulnerability that might apply to the TSF is reviewed to determine if there is a vulnerability that can be exploited in the TSF. For each vulnerability that could be exploited in the TSF, the vulnerability is treated as a bug requiring immediate remedy and work begins immediately to remedy the problem. Customers are informed of the vulnerability as described in the Life Cycle Support (ALC_FLR.2) Flaw Remediation submission; EROBUG10 – Innovation Data Processing Software Product Life Cycle Maintenance Support (Bug Track) User Guide, using the INNOVATION "News via Email" service and additionally, in the case of a security vulnerability as a further precaution, the "contact" at all effected customer sites is sent a notice by US Postal Service regular mail and a patch or maintenance version is released as soon as it is available.

These activities are documented in the following Vulnerability Assessment submission:

- EROVUL11 – FDRERASE/OPEN Vulnerability Assessment

The Vulnerability assessment assurance measure satisfies the following assurance requirements:

- 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;
- Security Assurance Requirements;
- Strength of Functions;
- Requirement Dependencies;
- TOE Summary Specification; and,
- PP Claims.

8.1 Security Objectives Rationale

This section shows that all secure usage assumptions and threats are completely covered by security objectives. In addition, each objective addresses or counters at least one assumption or threat.

	T.Data_remains_after_clear	T.Data_remnants_remain_after_sanitize	T.Data_scavenging	T.Errant_overwrite	T.Incomplete_overwrite	T.Unauthorized_use	T.Unattended_TOE
O.Authenticated_use						X	X
O.Erase_clears	X						
O.Record_of_operation				X	X		
O.Secure_erase_sanitizes		X	X				
O.Verified_operation				X			
OE.Operational_procedures				X			

Table 4: Threats to Objectives Correspondence

8.1.1 T.Data_remains_after_clear

Any person with programmatic access to the OS can access data on disk storage through programmatic means after the disk storage has been cleared.

This threat is countered by the TOE security objective O.Erase_clears. This objective will ensure the TOE erases all data on the target disk storage, rather than just logically removing the data (e.g., by simply deleting directory entries).

8.1.2 T.Data_remnants_remain_after_sanitize

Any person can access data remaining on disk storage after the disk storage has been sanitized, through programmatic means or specialized off-line and off-site attempts to recover data from electro-magnetic remnants of recorded data.

This threat is countered by the TOE security objective O.Secure_erase_sanitizes. This objective will ensure the TOE securely erases all data on the target disk storage such that it cannot be: read through programmatic means; retrieved using off-line or sophisticated laboratory techniques applied to hard drives removed from the control unit.

8.1.3 T.Data_scavenging

Any person with physical or programmatic access to disk storage that has been overwritten can exploit predictable overwrite patterns to analytically recover data from it.

This threat is countered by the TOE security objective O.Secure_erase_sanitizes. This objective will ensure the TOE securely erases all data on the target disk storage such that it cannot be: read through programmatic means; retrieved using off-line or sophisticated laboratory techniques applied to hard drives removed from the control unit.

8.1.4 T.Errant_overwrite

The TOE user invokes the TOE to overwrite disk storage with an inappropriate erase function, thus leaving the data that was on the disk storage at an unacceptable risk of compromise.

This threat is countered by the TOE security objectives O.Verified_operation and O.Record_of_operation, supported by the environment security objective OE.Operational_procedures. The objective O.Verified_operation ensures the TOE can be invoked to verify that a target disk volume has been completely overwritten. The objective O.Record_of_operation records every erase function performed on every disk drive, identifying the type of function (ERASE or SECUREERASE) and the parameters specified in the erase operation. This will provide the TOE user with the information necessary to determine if the appropriate erase function has been applied to the target disk storage. The objective OE.Operational_procedures supports O.Verified_operation, since the verify function is not automatic and local procedures may be required to ensure erased disk storage is subsequently verified.

8.1.5 T.Incomplete_overwrite

Unbeknownst to the TOE user, the TOE fails to completely overwrite disk storage, due to write failures, partial overwrites, or the disk storage being on-line and accessible to another program, thus resulting in data remaining on the disk storage when the TOE user believes it is completely erased.

This threat is countered by the TOE security objective O.Record_of_operation. This objective will ensure that the TOE generates a record of the result of each erase function performed on each disk volume. The report will identify if the erase function completed successfully (i.e., no data remains on the disk storage), or, if it did not complete successfully, the reason the function did not complete. The TOE user will therefore be able to determine the result of all requested erase functions.

8.1.6 T.Unauthorized_use

An unauthorized user obtains the TOE CD-ROM and its associated key device and uses it to erase disks without appropriate authority.

This threat is countered by the TOE security objective O.Authenticated_use. This objective will ensure that the TOE requires the user to authenticate to the TOE before allowing the user to interact with the TOE. The authentication provided by the user demonstrates the user is authorized to use the TOE. By requiring this authentication, the TOE provides a mechanism that reduces the risk that an unauthorized user can destroy user or system data simply by gaining access to the TOE CD-ROM and its associated key device.

8.1.7 T.Unattended_TOE

An unauthorized user interferes with the operation of the TOE left unattended by its authorized user, in order to erase disks without appropriate authority, change the TOE to employ an inappropriate erase function or prevent authorized erasure.

This threat is countered by the TOE security objective O.Authenticated_use. This objective will ensure that the TOE requires the user to re-authenticate to the TOE when an authenticated user locks access to the TOE security functions or, if the TOE detects user inactivity for a user-specified number of minutes, which could indicate the TOE has been left unattended. The authentication provided by the user demonstrates the user is authorized to use the TOE. This reduces the risk that an unauthorized user comes upon an unattended TOE and attempts to interfere with its operation, either by canceling erase operations in progress or by directing the TOE to erase disks that are not otherwise intended for erasure.

	A.Authorized_use	A.Competent_administration	A.Competent_use	A.Disk_volumes__not accessible	A.Secure_environment	A.Proper_procedures	A.Reliable_clock
OE.Authorized_use	X						
OE.Competent_staff		X	X	X	X		
OE.Controlled_facility					X		
OE.Operational_procedures						X	
OE.Reliable_clock							X

Table 5: Assumptions to Objectives Correspondence

8.1.8 A.Authorized_use

Any person with knowledge of the authentication password and/or the twenty-four character string Customer Key (FDRERASE/OPEN Key) and possession of the FDRERASE/OPEN CD/DVD and the USB flash drive is authorized to install and or use the TOE. Furthermore, an authorized user is authorized to view all information stored on the disk storage systems to be erased.

This assumption is satisfied by the environment security objective OE.Authorized_use. This objective will ensure that only those users that are authorized to use the TOE will have knowledge of the authentication password and the twenty-four character Customer Key and possession of the FDRERASE/OPEN CD/DVD and USB flash drive. Furthermore, this objective will ensure that authorized users are authorized to view all data stored on the disk storage system to be erased. This is necessary, since the TOE includes a function allowing the user to view the content of any disk sector before invoking the ERASE or SECUREERASE function.

8.1.9 A.Competent_administration

The persons responsible for administration of the TOE environment and installation of the TOE are trusted, trained, competent, and follow all applicable guidance documentation.

This assumption is satisfied by the environment security objective OE.Competent_staff. This objective will ensure the administrative staff of the TOE environment are trusted, trained, competent, and follow all applicable guidance.

8.1.10 A.Competent_use

The persons responsible for execution of the TOE are trusted, trained, competent, and follow all applicable guidance documentation.

This assumption is satisfied by the environment security objective OE.Competent_staff. This objective will ensure the users of the TOE are trusted, trained, competent, and follow all applicable guidance.

8.1.11 A.Disk_volumes_not accessible

All disks being overwritten are not accessible by any other systems or user programs. That is, all the disks honor/support the hardware reserve command or appropriate procedures in the IT environment ensure the disks being overwritten are unmounted to other systems.

This assumption is satisfied by the environment security objective OE.Competent_staff. This objective will ensure the administrative staff of the TOE environment and the users of the TOE will follow all applicable guidance. The guidance documentation for the TOE provides clear instructions to ensure all disks to be overwritten are unmounted (offline) on all other systems, and therefore not accessible by user programs. In particular, SATA disk volumes must not be physically connected to any computers other than the TOE host.

8.1.12 A.Secure_environment

The processing resources of the TOE will be located within controlled access facilities that will prevent unauthorized physical access. Furthermore, the underlying hardware environment operates correctly and is configured to support the operation of the TOE.

This assumption is satisfied by the environment security objectives OE.Competent_staff and OE.Controlled_facility. The objective OE.Competent_staff, by ensuring the TOE environment administrative staff follows applicable guidance, also ensures the underlying hardware environment is correctly configured according to the instructions in the guidance documentation. The objective OE.Controlled_facility ensures the TOE and its processing resources are protected from unauthorized physical access.

8.1.13 A.Proper_procedures

TOE users will abide by all higher authority directives, which could include a second person use of the TOE to verify the person executing the TOE overwrite operation did so on the intended disks, employing appropriate overwrite options.

This assumption is satisfied by the environment security objective OE.Operational_procedures. This objective will ensure the capabilities of the TOE, including the capability to verify an erase function, will be utilized in accordance with any higher authority directives or operational procedures.

8.1.14 A.Reliable_clock

The TOE operating environment includes a reliably functioning clock and issues a warning if there is no reliably functioning clock or the clock fails.

This assumption is satisfied by the environment security objective OE.Reliable_clock. This objective will ensure the IT environment provides a reliably functioning clock and issues a warning if there is no reliably functioning clock or the clock fails.

8.2 Security Functional Requirements Rationale

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

	O.Authenticated_use	O.Erase_clears	O.Record_of_operation	O.Secure_erase_sanitizes	O.Verified_operation	OE.Reliable_clock
FAU_GEN.1			X		X	
FAU_SAR.1			X		X	
FAU_STG.1			X			
FCS_COP.1	X					
FDP_BDE_EXP.1		X				
FDP_SDE_EXP.1				X		
FDP_DEV_EXP.1					X	
FIA_UAU.2	X					
FIA_UAU.6	X					
FMT_SMF.1		X		X	X	
FPT_RVM.1		X		X	X	
FPT_SEP.1		X		X	X	
FPT_STM.1						X
FTA_SSL.1	X					
FTA_SSL.2	X					

Table 6: Objectives to Requirements Correspondence

8.2.1 O.Authenticated_use

> *The TOE shall require a user to authenticate to the TOE prior to allowing the user to interact with the TOE and shall allow authenticated users to lock the TOE preventing unauthenticated users access to the TOE security functions. Furthermore, the TOE shall lock the user's interactive session if it does not detect any user activity for a user specified number of minutes, and shall require authentication in order to unlock the user session.*

This TOE security objective is satisfied by the TOE security functional requirement FIA_UAU.2, FTA_SSL.1 and FTA_SSL.2, supported by FIA_UAU.6 and FCS_COP.1.

FIA_UAU.2 specifies the requirement that the user is successfully authenticated before any other TSF-mediated actions can be performed on behalf of that user. FTA_SSL.1 specifies the requirement that the TSF lock the interactive session with the user after a number of minutes (specified by the user) of user inactivity, and that the user must re-authenticate in order to unlock the interactive session. FTA_SSL.2 specifies the requirement that the TSF allow the user to initiate locking of the user's own interactive session. FIA_UAU.6 supports the other requirements by requiring re-authentication in order to change the user password (thus ensuring only the authorized user can change the password) and to unlock the user's interactive session. FCS_COP.1 supports FIA_UAU.2 by providing a means for protecting the stored authentication data, through use of a non-reversible cryptographic hash mechanism.

8.2.2 O.Erase_clears

The TOE shall provide a capability to erase all data on disk storage so as to make the data inaccessible to an operating system user running a non-authorized or authorized program attempting to read the original data, running anywhere that has access to the disk storage.

This TOE security objective is satisfied by the TOE security functional requirement FDP_BDE_EXP.1, supported by FMT_SMF.1, FPT_RVM.1, and FPT_SEP.1.

FDP_BDE_EXP.1 specifies the requirement that selected disk volumes be overwritten at least once with a string of binary zeroes. This requirement provides the capability to erase all data on a disk storage system. FMT_SMF.1 provides the capability to select the appropriate overwrite operation to erase the data. FPT_RVM.1 ensures the erase function is invoked and cannot be bypassed, while FPT_SEP.1 ensures the TOE is protected from interference and tampering by untrusted subjects.

8.2.3 O.Record_of_operation

The TOE shall provide to the user a record of its operation for each overwrite function. Upon completion of an overwrite function, the TOE shall provide a record of the overwrite function used, the disk overwritten and the status of the overwrite results for each disk volume overwritten. The record will indicate if the overwrite was successful or unsuccessful. Furthermore, the TOE shall report to the user, during the progress of an overwrite function, the following occurrences that indicate the overwrite may not be successful: write failures to the disk; other I/O failures to the disk; cancellation of the security function.

This TOE security objective is satisfied by the TOE security functional requirements FAU_GEN.1 and FAU_SAR.1, supported by FAU_STG.1

FAU_GEN.1 specifies the requirement for generation of an audit record of the execution of the erase functions, indicating the success or failure of the functions. FAU_SAR.1 provides the TOE user with the capability to review the records of all overwrite operations performed by the TOE on all devices. FAU_STG.1 ensures that the records of overwrite operations are protected from unauthorized modification or deletion.

8.2.4 O.Secure_erase_sanitizes

The TOE shall provide a capability to securely erase all data on a disk so as to make the data inaccessible: to an operating system user running a non-authorized or authorized program attempting to read the original data, running anywhere that has access to the disk; through the use of off-line special tools designed to perform data recovery or by sophisticated laboratory techniques applied to hard drives removed from the control unit.

This TOE security objective is satisfied by the TOE security functional requirement FDP_SDE_EXP.1, supported by FMT_SMF.1, FPT_RVM.1, and FPT_SEP.1.

FDP_SDE_EXP.1 specifies the requirement that selected disk volumes be overwritten at least three times with a random data followed by its complement. This requirement provides the capability to securely erase all data on a disk storage system. FMT_SMF.1 provides the capability to select the appropriate overwrite operation to erase the data such that it is not recoverable even by sophisticated laboratory techniques. FPT_RVM.1 ensures the erase function is invoked and cannot be bypassed, while FPT_SEP.1 ensures the TOE is protected from interference and tampering by untrusted subjects.

8.2.5 O.Verified_operation

When the TSF has completed an erase function, there is significant assurance that the erase function has performed appropriately and overwritten every sector on the disk storage. The TOE shall provide a capability to verify that disk storage has been properly erased.

This TOE security objective is satisfied by the TOE security functional requirements FDP_DEV_EXP.1 and FAU_GEN.1, supported by FAU_SAR.1, FMT_SMF.1, FPT_RVM.1, and FPT_SEP.1.

FDP_DEV_EXP.1 specifies the requirement for a capability to verify that every sector of the specified disk storage has been overwritten with the appropriate pattern to make the data unrecoverable to the desired extent (dependent on the perceived risk of compromise). FAU_GEN.1 specifies the requirement for generation of an audit record of the execution of the verify function, indicating the success or failure of the function. FAU_SAR.1 specifies the capability for the TOE user to review the records of all verify operations performed by the TOE on all devices. FMT_SMF.1 specifies the requirement to provide the capability to verify that data on the disk storage has been successfully overwritten. FPT_RVM.1 ensures the verify function is invoked and cannot be bypassed, while FPT_SEP.1 ensures the TOE is protected from interference and tampering by untrusted subjects.

8.2.6 OE.Reliable_clock

The IT environment will provide a reliably functioning clock and will issue a warning if there is no reliably functioning clock or the clock fails.

This security objective for the IT environment is satisfied by the IT environment security functional requirement FPT_STM.1, which specifies the requirement to provide reliable time stamps. The time stamps will be deemed reliable if they are generated from a reliably functioning clock, and if the IT environment issues a warning if there is no reliably functioning clock or if the clock fails.

8.3 Security Assurance Requirements Rationale

The target assurance level is EAL2, augmented with ALC_FLR.2.

EAL2 was selected as the base assurance level because the TOE is a commercial product whose users require a low to moderate level of independently assured security. FDRERASE/OPEN is targeted at a relatively benign environment with good physical access security and competent TOE administrators and users. Within such environments, it is assumed that attackers will have a low attack potential. As such, EAL2 is appropriate to provide the assurance necessary to counter the limited potential for attack.

ALC_FLR.2 is selected as an appropriate augmentation because flaw remediation procedures provide greater assurance that security-related bugs will be fixed in a widely distributed commercial product.

8.4 Strength of Functions Rationale

The overall strength of function claim of SOF-basic is considered to be commensurate with the target assurance claim for the TOE of EAL2 (augmented with ALC_FLR.2) and the assumed environment of use of the TOE, as characterized in Section 3 of this ST. As discussed in Section 8.3 above, it is assumed potential attackers in this environment will have a low attack potential, and so SOF-basic represents an appropriate minimum strength of function claim. The only applicable security function is Authentication, which requires the user to enter a password to authenticate to the TOE prior to accessing any other TOE functionality, and also to re-authenticate in order to unlock an interactive session following a period of inactivity or when the user has specifically locked their interactive session. As identified in section 5.1, FIA_UAU.2 is the only specific TOE SFR for which an explicit strength of function claim is appropriate. Note that FTA_SSL.1 and FTA_SSL.2 do not specify an additional authentication mechanism, but simply rely on the mechanism specified by FIA_UAU.2, as demonstrated by the CC dependency of FTA_SSL.1 and FTA_SSL.2 on FIA_UAU.2.

8.5 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
FAU_GEN.1	FPT_STM.1	FPT_STM.1
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
FAU_STG.1	FAU_GEN.1	FAU_GEN.1

ST Requirement	CC Dependencies	ST Dependencies
FCS_COP.1	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4, FMT_MSA.2	See dependency rationale
FDP_BDE_EXP.1	none	none
FDP_SDE_EXP.1	none	none
FDP_RIV_EXP.1	none	FDP_BDE_EXP.1, FDP_SDE_EXP.1
FIA_UAU.2	FIA_UID.1	See dependency rationale
FIA_UAU.6	none	none
FMT_SMF.1	none	none
FPT_RVM.1	none	none
FPT_SEP.1	none	none
FTA_SSL.1	FIA_UAU.1	FIA_UAU.2
FPT_STM.1	none	none
ACM_CAP.2	none	none
ADO_DEL.1	none	none
ADO_IGS.1	AGD_ADM.1	AGD_ADM.1
ADV_FSP.1	ADV_RCR.1	ADV_RCR.1
ADV_HLD.1	ADV_FSP.1, ADV_RCR.1	ADV_FSP.1, ADV_RCR.1
ADV_RCR.1	none	none
AGD_ADM.1	ADV_FSP.1	ADV_FSP.1
AGD_USR.1	ADV_FSP.1	ADV_FSP.1
ALC_FLR.2	none	none
ATE_COV.1	ADV_FSP.1, ATE_FUN.1	ADV_FSP.1, ATE_FUN.1
ATE_FUN.1	none	none
ATE_IND.2	ADV_FSP.1, AGD_ADM.1, AGD_USR.1, ATE_FUN.1	ADV_FSP.1, AGD_ADM.1, AGD_USR.1, ATE_FUN.1
AVA_SOF.1	ADV_FSP.1, ADV_HLD.1	ADV_FSP.1, ADV_HLD.1
AVA_VLA.1	ADV_FSP.1, ADV_HLD.1, AGD_ADM.1, AGD_USR.1	ADV_FSP.1, ADV_HLD.1, AGD_ADM.1, AGD_USR.1

Table 7: TOE Security Requirement Dependencies

Part 2 of the Common Criteria specifies the following requirement dependencies that are not satisfied by this Security Target:

- FCS_COP.1 on [FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4, and FMT_MSA.2—These dependencies are all related to key management aspects of cryptography to support the claimed cryptographic operation: FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 for import or generation of keys; FCS_CKM.4 for destruction of keys; and FMT_MSA.2 to ensure secure values for cryptographic security attributes. However, the only cryptographic operation claimed for the TOE is secure hashing using SHA-1, which is a keyless operation. Therefore, none of these requirements are necessary.
- FIA_UAU.2 on FIA_UID.1—This dependency exists in the Common Criteria because it is usually expected that users will have to authenticate any identity they attempt to establish when interacting with the TSF. In the case of the FDRERASE/OPEN TOE, the TSF does identify individual users. It is an assumption of the intended use of the TOE that only users authorized to use the TOE will have knowledge of the TOE authentication data and possession of the FDRERASE/OPEN key (the USB flash drive). Therefore, since the purpose of the authentication requirement in this ST is to authenticate that a user is authorized to use the TOE, rather than to authenticate a user's claimed identity, FIA_UID.1 is not required.

8.6 Explicitly Stated Requirements Rationale

This Security Target specifies the following explicitly stated requirements: FDP_BDE_EXP.1; FDP_SDE_EXP.1; and FDP_DEV_EXP.1.

FDP_BDE_EXP.1 and FDP_SDE_EXP.1 specify unique requirements for the product type of the TOE that are not covered by any security functional requirement in Part 2 of the Common Criteria. The TOE type is a data erasure

product and the TOE is intended for a specific environment (an x86 architecture computer system configured to support Solaris 10) and specific data storage devices (IBM, EMC, and Hitachi Data disk storage systems). The CC provides the Residual Information Protection (FDP_RIP) family within the User Data Protection (FDP) class of security functional requirements to address the need to ensure that deleted information is no longer accessible. However, the FDP_RIP family of requirements is intended to specify the need to ensure that information deleted from resources within the TOE Scope of Control is no longer accessible and that newly created objects do not contain information from previously used objects within the TOE. The "objects" that are the target of FDRERASE/OPEN are not objects that come within its scope of control, but rather are residual objects of another IT entity (such as an operating system). These objects and their information may still be considered to exist within the scope of the other IT entity, if that entity were to be currently active (e.g., data files may not have been deleted from the operating system's file system). As such, FDRERASE/OPEN does not meet the intent of the FDP_RIP family of requirements, and so FDP_BDE_EXP.1 and FDP_SDE_EXP.1 have been explicitly stated to specify the requirements for basic (the ERASE function) and secure (the SECURE ERASE function) disk erasure capabilities.

FDP_DEV_EXP.1 specifies a unique requirement for the product type of the TOE that is not covered by any security functional requirement defined in Part 2 of the Common Criteria. The CC does not provide a requirement to verify that information that should have been erased from a disk volume has in fact been erased. One objective of the TOE is to provide the user appropriate assurance that the data that was on a disk storage system has been made inaccessible, commensurate with the perceived level of risk. For example, the user may wish to dispose of the disk storage system and wants to be confident that all data previously stored on the disk storage system has been erased sufficiently that its recovery is impractical if the disk storage system should end up "in the wrong hands". FDP_DEV_EXP.1 has been specified to address the need for such a verification capability in the TOE product type.

FDP_DEV_EXP.1 has a dependency on FDP_BDE_EXP.1 and FDP_SDE_EXP.1, since it would be meaningless to attempt to verify that a disk had been erased if there was no requirement to erase a disk. This dependency is identified in Table 6.

8.7 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.

	Security audit	User data protection	Authentication	Security management	Protection of the TSF
FAU_GEN.1	X				
FAU_SAR.1	X				
FAU_STG.1	X				
FCS_COP.1			X		
FDP_BDE_EXP.1		X			
FDP_SDE_EXP.1		X			
FDP_DEV_EXP.1		X			
FIA_UAU.2			X		
FIA_UAU.6			X		
FMT_SMF.1				X	
FPT_RVM.1					X

FPT_SEP.1					X
FTA_SSL.1			X		
FTA_SSL.2			X		

Table 8: Security Functions vs. Requirements Mapping

8.8 PP Claims Rationale

See Section 7, Protection Profile Claims.