National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

Innovation Data Processing

FDRERASE/OPEN, Version 02, Level 05

Report Number: CCEVS-VR-VID10232-2008
Dated: **29 January 2008**
Version: **3.0**

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6740
Fort George G. Meade, MD 20755-6740

ACKNOWLEDGEMENTS

Validation Team

Deb Downs, Senior Validator, Aerospace
Jenn Dotson, Lead Validator, Aerospace

Common Criteria Testing Laboratory

Terrie Diaz, Lead Evaluator
Science Applications International Corporation (SAIC)
Columbia, Maryland

Table of Contents

1 Executive Summary

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Innovation Data Processing FDRERASE/OPEN Version 0.2, Level 05. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied.

The evaluation of Innovation Data Processing FDRERASE/OPEN Version 0.2, Level 05 was performed by Science Applications International Corporation (SAIC) Common Criteria Testing Laboratory in the United States and was completed on 6 December 2007.

The information in this report is largely derived from the Security Target (ST), Evaluation Technical Report (ETR) and associated test report. The ST was written by SAIC. The ETR and test report used in developing this validation report were written by SAIC. The evaluation team determined the product to be Part 2 extended and Part 3 conformant, and meets the assurance requirements of EAL 2 augmented with ALC_FLR.2. The product is not conformant with any published Protection Profiles. All security functional requirements are derived from Part 2 of the Common Criteria or expressed in the form of Common Criteria Part 2 requirements.

The TOE is FDRERASE/OPEN Version 0.2, Level 05 provided by Innovation Data Processing, Inc. The TOE is an application and supporting operating system that is 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 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 ensure data is physically written to disk and to confirm that erasure did take place.

The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence adduced. This Validation Report is not an endorsement of the Innovation Data Processing FDRERASE/OPEN Version 0.2, Level 05 product by any agency of the US Government and no warranty of the product is either expressed or implied.

During this validation, the Validators monitored the activities of the SAIC evaluation team, provided guidance on technical issues and evaluation processes, reviewed successive versions of the Security Target, reviewed selected evaluation evidence, reviewed test plans, reviewed intermediate evaluation results (i.e., the CEM work units), and reviewed

successive versions of the ETR and test reports. The Validator determined that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements defined in the Security Target (ST). Therefore, the Validator concludes that the SAIC findings are accurate, the conclusions justified, and the conformance claims correct.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through EAL 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation conduct security evaluations.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products, desiring a security evaluation, contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated;
- The Security Target (ST), describing the security features, claims, and assurances of the product;
- The conformance result of the evaluation;
- The Protection Profile to which the product is conformant; and
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE:	Innovation FDRERASE/OPEN Version 0.2, Level 05
Protection Profile	Not applicable.
ST:	Innovation FDRERASE/OPEN Version 0.2, Level 05 Security Target, Version 1.0, 24 January 2008
Evaluation Technical Report	Evaluation Technical Report for Innovation FDRERASE/OPEN Version 0.2 Level 05, Part 1 (Non-Proprietary, Version 1.0 13 December 2007, Part 2 (Proprietary), Version 1.0 18 December 2007

Item	Identifier
CC Version	Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005
Conformance Result	CC Part 2 extended and Part 3 conformant, EAL 2 augmented with ALC_FLR.2
Sponsor	Innovation Data Processing
Developer	Innovation Data Processing
Common Criteria Testing Lab (CCTL)	Science Applications International Corporation (SAIC), Columbia, MD
CCEVS Validator	The Aerospace Corporation

3 Organizational Security Policy

Innovation FDRERASE/OPEN Version 0.2 Level 05 provides security functions related to the secure erasure of data. Specifically, the TOE supports two grades[1] of secure erasure:

1. "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.
2. "SECURE ERASE": 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.

In addition, there is a "VERIFY" function, which samples 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.

[1] Extracted from SAIC ETR Part 1 Version 2.0, 28 January 2008

4 Assumptions and Clarification of Scope

The statement of TOE security environment describes the security aspects of the environment in which it is intended that the TOE will be used and the manner in which it is expected to be employed. The statement of TOE security environment therefore identifies the assumptions made on the operational environment and the intended method for the product, defines the threats that the product is designed to counter and the organizational security policies which the product is designed to comply.

Following are the assumptions identified in the Security Target:

- It is assumed that 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.
- It is assumed that the persons responsible for administration of the TOE environment and installation of the TOE are trusted, trained, competent, and follow all applicable guidance documentation.
- It is assumed that the persons responsible for execution of the TOE are trusted, trained, competent, and follow all applicable guidance documentation. Note: Since it is assumed administrators are trusted, the administrative actions (e.g. changing the password) are not audited.
- It is assumed that 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.
- It is assumed that the processing resources of the TOE will be located within controlled access facilities that will prevent unauthorized physical access. Furthermore, the underlying hardware and operating system software environment operates correctly and is configured to support the operation of the TOE.
- It is assumed that 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.
- It is assumed that the TOE operating environment includes a reliably functioning clock and issues a warning if there is no reliably functioning clock or the clock fails.

Following are the threats levied against the TOE and its environment as identified in the Security Target. The threats that are identified are mitigated by the TOE and its environment. All of the threats identified in the ST are addressed.

- Any person with programmatic access to the OS can access data on disk storage through programmatic means after the disk storage has been cleared.
- 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.
- 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.
- 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.
- 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.
- An unauthorized user obtains the TOE CD-ROM and its associated key device and uses it to erase disks without appropriate authority.
- 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.

The TOE 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.

5 Architectural Information[2]

This section provides a high level description of the TOE and its components as described in the Security Target.

The physical components of FDRERASE/OPEN consist of:

- 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.

[2] Extracted from SAIC ETR Part 1 Version 1.0, 13 December 2007

- 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 will contain the "FDRERASE/OPEN key".

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).

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.

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

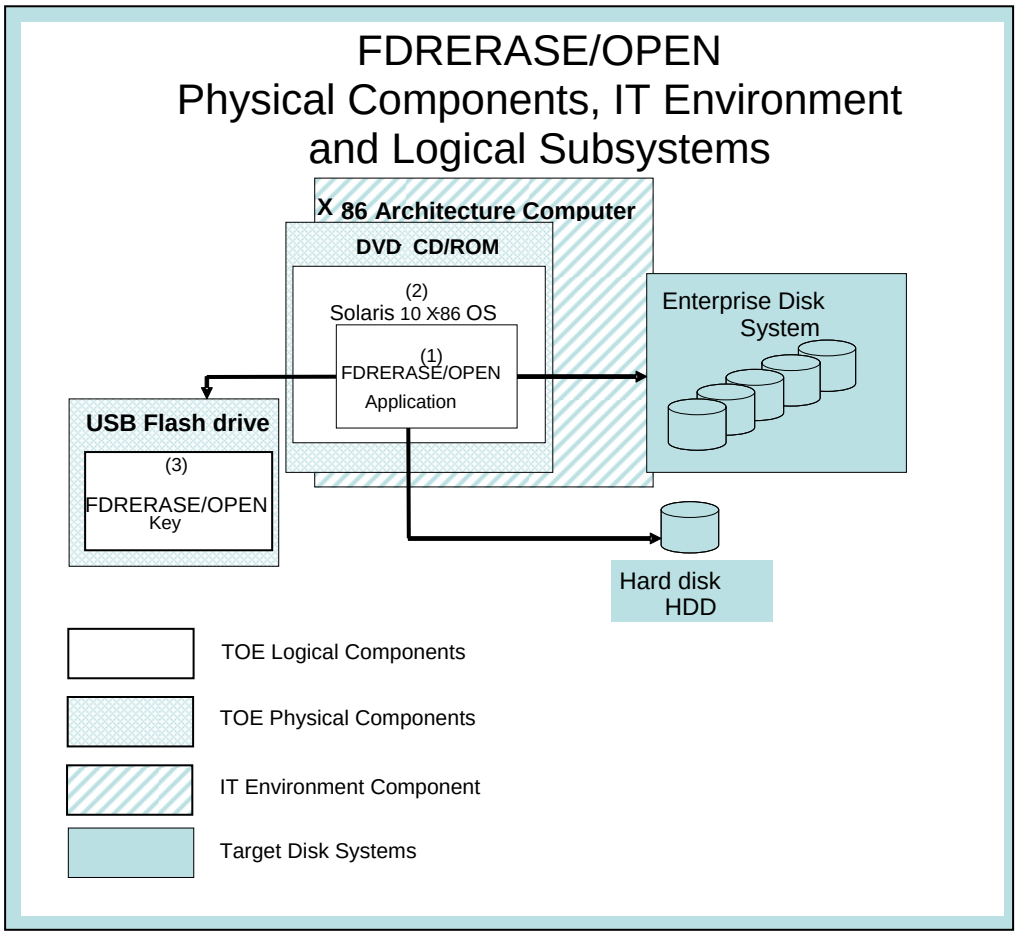

Figure 1 TOE and IT environment Components

6 Documentation

Following is a list of the evaluation evidence, each of which was issued by the developer (and sponsor).

Design documentation

Document	Version	Date
INNOVATION Data Processing FDRERASE/OPEN Solution Functional Specification, High-Level Design and Representation Correspondence Document	ERODES15	28 January 2008

Guidance documentation

Document	Version	Date

Document	Version	Date
INNOVATION Data Processing FDRERASE/OPEN User Manual and Installation Guide	ERODOC25.9	January 2008
Guidance (AGD) Resubmission Letter IV and Attachment For Evidence Element AGD_ADM.1 and AGD_USR.1	Resubmission Letter IV	28 January 2008

Configuration Management documentation

Document	Version	Date
INNOVATION Data Processing FDRERASE/OPEN Solution Configuration Management Developer Guide	EROCFM11	12/20/2007

Delivery and Operation documentation

Document	Version	Date
INNOVATION Data Processing Software Distribution Process Description and Software Distribution Facility User Guide	ERSDOP14	9/7/2007
Delivery and Operation (ADO) Resubmission Letter II and Attachment For Evidence Elements ADO_DEL.1 and ADO_IGS.1 Innovation Data Processing, Inc. FDRERASE/OPEN V2.5	Resubmission Letter II	7 September 2007

Life Cycle Support documentation

Document	Version	Date
INNOVATION Data Processing FDRERASE/OPEN Solution Software Product Life Cycle Maintenance Support User Guide	EROBUG13	August 2007
Software Product Life Cycle Maintenance Support (ALC) Resubmission Letter 2 and Attachment (EROBUG13) for Evidence Element ALC_FLR.2 Innovation Data Processing, Inc. FDRERASE/OPEN V2.5	Resubmission Letter 2	August 10, 2007

Test documentation

Document	Version	Date
INNOVATION Data Processing FDRERASE/OPEN	EROATE13	01/24/2008

Document	Version	Date
Solution Testing Procedures and Test Documentation		
INNOVATION Data Processing FDRERASE/OPEN Test Cases (ERASEO0001, ERASEO0002,ERASEO0003, ERASEO0003A, ERASEO0003B, ERASEO0003C, ERASEO0004, ERASEO0005, ERASEO0005A, ERASEO0006, ERASEO0007, ERASEO0008, ERASEO0009, ERASEO0010, ERASEO0010A, ERASEO0011, ERASEO0012, ERASEO0013, ERASEO0013A, ERASEO0013C, ERASEO0014 , ERASEO0015, ERASEO0015A, ERASEO0015B, ERASEO0016, ERASEO0017, ERASEO0017C, ERASEO0018, ERASEO0019, ERASEO0020, ERASEO0021, ERASEO0022, ERASEO0023, ERASEO0023A, ERASEO0023C, ERASEO0024, ERASEO0025, ERASEO0026, ERASEO0027, ERASEO0028, ERASEO0029, ERASEO0030, ERASEO_PART1, ERASEO_PART2, ERASEO_STARTUP, ERASEO_EXCL_ACCESS, and ERASEO_USBFULL)		12/4/2007 through 01/25/2008
Tests (ATE) Resubmission Letter III With Attachment for Evidence Elements ATE_COV.1, ATE_FUN.1 and ATE_IND.2 Innovation Data Processing, Inc. FDRERASE/OPEN V2.5	Resubmission Letter III	December 11, 2007

The actual results are contained within numerous the test cases, log, and history files and were copied to a CD that was submitted to the evaluation team.

Vulnerability Assessment documentation

Document	Version	Date
INNOVATION Data Processing FDRERASE/OPEN Vulnerability Assessment	EROVUL11	10/29/2007
Vulnerability Assessment (AVA) Resubmission Letter I and Attachment For Evidence Element AVA_VLA.1 Innovation Data Processing, Inc. FDRERASE/OPEN V02.05	Resubmission Letter I	October 29, 2007

Security Target

Document	Version	Date
Innovation Data Processing FDRERASE/OPEN Security Target	1.0	24 January 2008

7 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team.

7.1 Developer Testing

The developer tested the interfaces identified in the functional specification and mapped each test to the security function tested. The scope of the developer tests included all the TSFI. The testing covered the security functional requirements in the ST including: Security audit, User data protection, Authentication, Security management, Protection of the TSF, and TOE access. The security function that was not covered by the developers testing was Cryptographic operation; hashing of the password. Since this is EAL2 complete coverage of the TSF is not required, however to demonstrate complete coverage of the TSF, the evaluation team developed test to ensure complete coverage of the TSF. The evaluation team determined that the developer's actual test results matched the vendor's expected results.

7.2 Evaluation Team Independent Testing

The evaluation team re-ran a subset of the vendor's tests against various drive types during testing. In addition to rerunning the vendor's tests, the Evaluation Team developed a set of independent team tests to address areas of the ST that did not seem completely addressed by the vendor's test suite, or areas where the ST did not seem completely clear. All were run as manual tests.

The vendor provided three machines connected to various enterprise storage systems containing SCSI and Fibre channel drives: EMC DMX3, IBM DS8100, and Hitachi 9970V. These drives were the subject of erasure.

The following hardware is necessary to create the test configuration: workstation/server. The following software is required to be installed on the workstation(s) used for the tests: The FDRERASE/OPEN application in a locked state, Solaris 10 OS, preconfigured to automatically start FDRERASE/OPEN after the boot of the OS is complete, and the FDRERASE/OPEN key which is provided on a USB flash drive, to unlock the associated FDRERASE/OPEN application. In addition, in order to run the tests; each individual test procedure/instructions are needed.

In addition to developer testing, the CCTL conducted its own suite of tests, which were developed independently of the sponsor. These also completed successfully.

7.3 Vulnerability Testing

The evaluators developed vulnerability tests to address the Protection of the TSF security function and the Authentication and TOE access SFRs, as well as expanding upon the public search for vulnerabilities provided to the team by the sponsor. These tests identified no vulnerabilities in the specific functions provided by the TOE.

8 Evaluated Configuration

The TOE consists of an application and supporting operating system that run on x86 architecture computers. The application and OS are loaded onto a computer from a CD-ROM compact disc by an authorized person. The Sun Solaris 10 operating system is pre-configured to automatically start FDRERASE/OPEN after the boot of Solaris 10 is complete. The method results in Solaris 10 invoking FDERASE/OPEN as the sole user application executing on the computer.

The TOE also consists of a USB flash drive which must be plugged in and must contain validation codes that match the CD-ROM. These codes are compared at startup and if they do not match the TOE start-up will not complete and therefore cannot be used. The USB flash drive is also used to store options, logs and history records.

The TOE is expected to be running in a physically secure environment, have a time of day clock function, be capable of supporting Solaris 10 and be connected by SCSI or Fibre channels to the disk storage systems to be erased. The host computer must contain a CD-ROM or DVD drive, a USB port, and a minimum of 512K of memory (1 GB is recommended).

The test machines consisted of:

- Dell Dimension 9200, Dell Dimension 4600 and Dell Power Edge 2550.

The test machines were connected to either SCSI or Fibre channel connections with the following disk volume drives:

- IBM DS8000 (2107) series subsystem
- EMC Symmetrix DMX3 series subsystem
- Hitachi (HDS) Lightning 9970V series subsystem

9 Results of the Evaluation

The evaluation was conducted based upon the Common Criteria (CC), Version 2.3, dated August 2005; the Common Evaluation Methodology (CEM), Version 2.3, dated August 2005; and all applicable International Interpretations in effect on November 2007. The evaluation confirmed that the Innovation FDRERASE/OPEN Version 0.2 Level 05 product is compliant with the Common Criteria Version 2.3, functional requirements (Part 2), Part 2 extensions, and assurance requirements (Part 3) for EAL2 augmented with ALC_FLR.2. The details of the evaluation are recorded in the CCTL's evaluation technical report; Final Evaluation Technical Report for the Innovation FDRERASE/OPEN Version 0.2 Level 05, Part 1 (Non-Proprietary) and Part 2 (Proprietary). The product was evaluated and tested against the claims presented in the Innovation FDRERASE/OPEN Version 0.2 Level 05 Security Target, Version 1.0, 24 January 2008.

The Validator followed the procedures outlined in the Common Criteria Evaluation Scheme publication number 3 for Technical Oversight and Validation Procedures. The Validator has observed that the evaluation and all of its activities were in accordance with

the Common Criteria, the Common Evaluation Methodology, and the CCEVS. The Validator therefore concludes that the evaluation team's results are correct and complete.

The following evaluation results are extracted from the non-proprietary Evaluation Technical Report provided by the CCTL.

9.1 Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of threats, policies, and assumptions, a statement of security requirements claimed to be met by the Innovation Data Processing, FDRERASE/OPEN, Version 02, Level 05 product that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

9.2 Evaluation of the Configuration Management Capabilities (ACM)

The evaluation team applied each EAL 2 augmented with ALC_FLR.2 ACM CEM work unit. The ACM evaluation ensured the TOE is identified such that the consumer is able to identify the evaluated TOE. The evaluation team ensured that configuration items are uniquely identified, and that documented procedures are used to control and track changes that are made to the TOE. In addition the evaluation team ensured changes to the implementation representation are controlled and that TOE associated configuration item modifications is properly controlled.

9.3 Evaluation of the Delivery and Operation Documents (ADO)

The evaluation team applied each EAL 2 augmented with ALC_FLR.2 ADO CEM work unit. The ADO evaluation ensured the adequacy of the procedures to deliver, install, and configure the TOE securely. The evaluation team ensured the procedures addressed identification of the TOE and allows for detection of unauthorized modifications of the TOE. The evaluation team followed the INNOVATION Data Processing Software Distribution Process Description and Software Distribution Facility User Guide and the INNOVATION Data Processing FDRERASE/OPEN User Manual and Installation Guide to receive the TOE and test the installation procedures to ensure the procedures result in the evaluated configuration.

9.4 Evaluation of the Development (ADV)

The evaluation team applied each EAL 2 augmented with ALC_FLR.2 ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification and high-level design documents. The evaluation team also ensured that the correspondence analysis between the design abstractions correctly demonstrated that the lower abstraction was a correct and complete representation of the higher abstraction.

9.5 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each EAL 2 augmented with ALC_FLR.2 AGD CEM work unit. The evaluation team ensured the adequacy of the guidance documents in describing

how to securely administer the TOE. The Software Distribution Facility User Guide and the INNOVATION Data Processing FDRERASE/OPEN User Manual and Installation Guide were assessed during the design and testing phases of the evaluation to ensure it was complete.

9.6 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied ALC_FLR.2 work units from the CEM supplement. The vendor's flaw remediation procedures documentation and flaw remediation guidance documentation was evaluated to determine whether the developer has established flaw remediation procedures that describe the tracking of security flaws, the identification of corrective actions, and the distribution of corrective action information to TOE users.

9.7 Evaluation of the Test Documentation and the Test Activity (ATE)

The Evaluation Team applied each EAL 2 augmented with ALC_FLR.2 ATE CEM work unit. The evaluation team ensured that the TOE performed as described in the design documentation and demonstrated that the TOE enforces the TOE security functional requirements. Specifically, the evaluation team ensured that the vendor test documentation sufficiently addresses the security functions as described in the functional specification and high level design specification. The evaluation team performed a complete test of the vendor's automated test suite, and devised an independent set of team test and penetration tests. The vendor tests, team tests, and penetration tests substantiated the security functional requirements in the ST.

9.8 Vulnerability Assessment Activity (AVA)

The Evaluation Team applied each EAL 2 augmented with ALC_FLR.2 AVA CEM work unit. The evaluation team ensured that the TOE does not contain exploitable flaws or weaknesses in the TOE based upon the developer vulnerability analysis and the evaluation team's vulnerability analysis, and the evaluation team's performance of penetration tests.

9.9 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's performance of a subset of the vendor tests suite, the independent tests, and the penetration tests also demonstrated the accuracy of the claims in the ST.

10 Validator Comments/Recommendations

All Validator concerns with respect to the evaluation have been addressed. No issues are outstanding.

The TOE is protected from unauthorized access to itself by the simple expedient of not providing internal access to its own executable: the only interfaces to the TOE are ERASE, SECUREERASE, and VERIFY, none of which can alter the TOE executable.

FDRERASE/OPEN is a particularly powerful tool that has the capability to erase all data from open system disk volumes. Anyone who has access to the FDRERASE/OPEN CD, the associated USB flash drive, customer key, and the current password has complete control of the FDRERASE/OPEN secure erasure tool. Also, 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.

It should be noted that the authentication password can not be reset unless the user is in possession of the current authentication password and is not recoverable if forgotten. If the password is forgotten, the only way to use the TOE is to clear all the information from the FDRERASE/OPEN USB flash drive and reinitialize the TOE with a valid 'customer key". INNOVATION can provide a replacement 'customer key'.

TOE users can also view and print the individual Disk Log Files and the cumulative History File that the TOE records on the FDRERASE/OPEN USB flash drive from Windows, or any other operating system that will mount a USB flash drive. It should be noted that the records may be modified and/or deleted. The Guidance documents provide warnings and procedures for securely handling the audit records (Logs and History files).

11 Security Target

The Security Target is identified as Innovation Data Processing FDRERASE/OPEN Security Target, Version 1.0, dated 24 January 2008. The document identifies the security functional requirements (SFRs) necessary to implement the TOE security policies. These include TOE SFRs and IT Environment SFRs. Additionally, the Security Target specifies the security assurance requirements necessary for EAL 2 augmented with ALC_FLR.2.

12 Glossary

The following definitions are used throughout this document:

ACL	Access Control Lists
CC	Common Criteria
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.
CM	Control Management
CPU	Central Processing Unit

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.
DO	Delivery Operation
EAL	Evaluation Assurance Level
EMC	An American Fortune 500 and S&P 500 manufacturer of software and systems for information management and storage. EMC is headquartered in Hopkinton, Massachusetts, USA
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
HDS	Hitachi Data Systems; Hitachi Data Systems Corporation, a subsidiary of Hitachi, with enterprise storage systems group based both in Japan and in Santa Clara, California, US
IBM	International Business Machines
I/O	Input/Output
JAVA	A programming language that provides the ability to create a GUI for dialog services.
PP	Protection Profile
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.
SF	Security Functions
SFR	Security Functional Requirement(s)
ST	Security Target

TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy
TSC	TSF Scope of Control
USB flash drive	A NAND-type flash memory data storage device integrated with a USB interface. They are typically small, lightweight, removable and rewritable.

13 Bibliography

The Validation Team used the following documents to produce this Validation Report:

[1] Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model, Version 2.3, August 2005.

[2] Common Criteria for Information Technology Security Evaluation - Part 2: Security Functional Requirements, Version 2.3, August 2005.

[3] Common Criteria for Information Technology Security Evaluation - Part 3: Security Assurance Requirements, Version 2.3, August 2005.

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 2.3, August 2005.

[5] Part 2: Evaluation Methodology, Supplement: ALC_FLR - Flaw Remediation, Version 1.1, February 2002, CEM-2001/0015R.

[6] Innovation Data Processing, FDRERASE/OPEN, Version 02, Level 05 FINAL Non-Proprietary ETR – Part 1.

[7] Innovation Data Processing, FDRERASE/OPEN, Version 02, Level 05 FINAL Proprietary ETR – Part 2 and Supplemental Team Test Plan.

[8] Innovation Data Processing FDRERASE/OPEN Security Target, Version 1.0, 24 January 2008.

[9] NIAP Common Criteria Evaluation and Validation Scheme for IT Security, Guidance to Common Criteria Testing Laboratories, Version 1.0, March 20, 2001.