SuperNet 2000 EAL4/r1 Common Criteria Security Target (EAL4)

Revision V2.0

Prepared for:

Electronic Engineering Systems, Inc.
1200 North Battlefield Boulevard, Suite 120
Chesapeake, VA 23320

Prepared by:

SAIC Center for Information Security Technology
7125 Columbia Gateway Drive, Suite 300
Columbia, MD 21046

October 20, 2000

TABLE OF CONTENTS

FIGURES

TABLES

1 REVISION HISTORY

This Section provides a mechanism to identify when specific versions of this document were released and also specifies what modifications were performed when moving from one version to the next.

Version	Date	Comments
1.0	08 July 2000	In itial draft
1.1	22 July 2000	Version delivered for CC evaluation
1.2	24 August 2000	Updated with evaluation team comments
1.3	28 August 2000	Final pre-evaluation updates
1.4	6 September 2000	Final pre-evalution editorial changes
2.0	2 October 2000	Post Chief Validator review

2 INTRODUCTION

This document is a Security Target (ST), as defined by the Common Criteria[1]. This ST describes a set of security requirements and specifications to be used as the basis for evaluation of an identified Information Technology (IT) product. The IT product described in this ST is the SuperNet 2000 EAL4/r1 developed by Electronic Engineering Systems Incorporated (EESI). The SuperNet 2000 EAL4/r1 components and associated administrator and user guidance documentation that are the subject of an evaluation are called the Target of Evaluation (TOE).

This ST identifies the environment appropriate for the SuperNet 2000 EAL4/r1 to operate within. In this operating environment, operating assumptions are identified that restrict the set of security threats. Threats associated with the SuperNet 2000 EAL4/r1 operating in an appropriate environment are identified, and the security functions that address these threats are identified. Finally, the ST describes how the TOE provides the security functions. In summary, this ST decomposes an operating environment and the IT threats associated with that environment to a TOE implementation.

The structure and contents of this ST comply with the requirements specified in the CC, Part 1, Annex C, and Part 3, Chapter 5. The TOE conforms to Parts 2 and 3 of the CC, Version 2.1 and provides an EAL 4 level of assurance.

2.1 ST and TOE Identification

The following summary information identifies this ST and the TOE:

Evaluation (TOE): the SuperNet 2000 EAL4/r1 (see Figure 1),
Evaluation Assurance Level: (EAL) 4,
ST Title: Electronics Engineering Systems Incorporated (EESI), SuperNet 2000 EAL4/r1 Security Target,
ST Version: 2.0,
TOE Identification: EESI SuperNet 2000 EAL4/r1,
CC Identification: Common Criteria for Information Technology Security Evaluation, Version 2.1, August 1999,
ST Evaluation: Science Applications International Corporation (SAIC)
Keywords:

This Security Target completely describes the Target of Evaluation (TOE), appropriate security environments, the security objectives, the security requirements met, and the functionality of the product. The structure and contents of this ST comply with the requirements specified in the CC, Part 1, Annex C, and Part 3, Chapter 5. This ST contains sections that address Security Environment, Security Objectives, and IT Security Requirements, as well as Security Objectives Rationale and Security Requirements Rationale sections.

The Security Target was written by SAIC acting on behalf of EESI and this ST will be evaluated by the Common Criteria Testing Laboratory of SAIC.

[1] International Standards organization (ISO) 1540-1, the Common Criteria for Information Technology Security Evaluation, Version 2.1, August 1999.

Figure 1 - SuperNet 2000 EAL4/r1

This Security Target describes the security features of the SuperNet 2000 EAL4/r1. The SuperNet 2000 EAL4/r1 separates two hardware domains within one workstation, where each domain provides access to a specific set of hardware devices that contain user data. Each hardware domain is called a user data domain (UDD), since devices that communicate with networks (nic) and devices used for storing user data (floppy and hard drives) are unique to each domain. One UDD, the public UDD, is accessible by all users who have physical access to the TOE, while the other UDD provides restricted access; therefore, one set of hardware devices is available to all users while another set of hardware devices has restricted access. Each UDD is selected through the use of a hardware switch. The hardware switch, or Domain Selection Switch (DSS), has default setting, in that when the TOE is not in use by a trusted user, the DSS always selects the public UDD. When a trusted user inserts a physical key into the DSS, the restricted UDD can be selected. The SuperNet 2000 EAL4/r1 provides this functionality at the Common Criteria "methodically designed, tested, and reviewed" assurance level, EAL 4.

2.2 Conventions

This section describes the conventions used to denote CC operations on security requirements and to distinguish text with special meaning. The notation, formatting, and conventions used in this ST are largely consistent with those used in the CC.

The CC allows several operations to be performed on functional requirements; assignment, iteration, refinement, and selection are defined in paragraph 2.1.4 of Part 2 of the CC.

The assignment operation identifies a data element or type of information, where the content of the element is to be specific to the product. An assignment is indicated by showing the value in square brackets with bold text [assignment: **a**].

The selection operation is used to identify an acceptable set of values from a predefined list for a specific requirement. Selection of security requirements is denoted with square brackets and bold Italics [selection: ***a, b, c***].

The refinement operation is used to identify a specific set of values that are used to narrow the scope of an element. Refinement is not used in this ST.

The iteration operation permits the use of a component more than once with varying operations.

There are no operations performed on the assurance requirements.

2.2.1 Terminology

2.2.1.1 Terminology specific for a Security Target

Security Target
This ST principally defines a set of assumptions about the security aspects of a TOE. The security aspects include the following:

- Environment in which the TOE must operate to be able to enforce the TSP (security context),
- Threats which the TOE is intended to counter (security perimeter),
- Security objectives and a set of security requirements (features) to address the threats (security scope),
- IT security functions provided by the Target of Evaluation (TOE) that provide the features that meet the security requirements (security content).

Internally consistent
There can be no apparent contradictions between any aspects of an entity in a Security Target. In terms of documentation, this means that there can be no statements within the documentation that can be taken to contradict each other.

Mutually supportive
A relationship must exist between a group of entities indicating that the entities possess properties, which do not conflict with, and may assist, the other entities in performing their tasks. It is not necessary to determine that every individual entity in question directly supports other entities in that grouping; rather, it is a more general determination that is made.

2.2.1.2 Terminology specific to the TOE

Hardware Domain
A hardware domain consists of hardware that receives electrical power to provide an operational workstation. A hardware domain is the interconnected usable hardware (including firmware), configured in one SuperNet 2000 EAL4/r1 system, that provides one platform to install and execute IT software.

Domain Selection Switch
The Domain Selection Switch (DSS) is the manual switch that is physically moved to select one UDD. The DSS is controlled by a secure DSS Key.

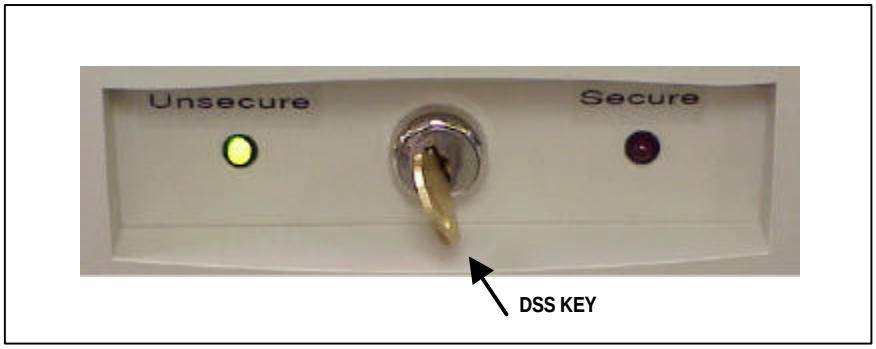

Figure 2 - Domain Selector Switch

DSS Key
A physical key inserted into the DSS to switch the DSS. The DSS cannot be switched without the DSS Key.

User Information
In this ST, user information is considered information that can be modified by a user. System information that can be modified only by an administrator is not considered user information.

User Data Domain
Each hardware domain is called a user data domain (UDD), since devices that communicate with networks (nic) and devices used for storing user data (floppy and hard drives) are unique to each domain. Only one UDD is available for use at any one time. Hardware that is part of the SuperNet 2000 EAL4/r1 that is isolated to a single UDD includes hard drives, network connections, and floppy drives. The TOE provides two UDDs; one is the unrestricted UDD and the other is the restricted UDD. When the TOE is not in operation, the DSS must select the unrestricted UDD.

Operational Device
An Operational Device is any hardware device within the SuperNet 2000 EAL4/r1 workstation that is receiving electrical power[2].

Restricted UDD
Also called the trusted UDD. The UDD selection position on the DSS that only can be selected by inserting a key into the DSS and turning the key.

Unrestricted UDD
UDD that is selected by the default DSS position. This is the only position in which the DSS can be if a physical key is not inserted into the DSS. Only trusted users may have access to a DSS Key and they are instructed never to leave the DSS Key in the DSS, therefore the DSS must be selecting the unrestricted UDD when the TOE is not in operation.

Role – A predefined set of rules establishing the allowed interactions between a user and the TOE. Four roles exist to install, maintain, and use the TOE. The roles are the "general user," "trusted user," "administrator," and the "installer."

General User
Any person who has physical access to the SuperNet 2000 EAL4/r1 and who does not possess a DSS Key.Upon approaching the TOE, the DSS is always in the position that selects the unrestricted UDD. A general user only has access to the unrestricted UDD.

Trusted User
Any person, who has in their possession a physical key necessary to switch the DSS into the "trusted" UDD, also called "restricted" UDD. A trusted user may access the unrestricted UDD and the restricted UDD. To access the restricted UDD, the trusted user must first insert a key into the DSS. To switch the DSS to the restricted UDD a trusted user inserts the key into the DSS and switches the DSS to the restricted UDD. When the user wishes to switch the DSS from the restricted to the unrestricted UDD, the key must be used, since the key cannot be removed from the DSS when the DSS is selecting the restricted UDD. The DSS key can be removed only in the unrestricted position. Users are instructed in the user manual to never leave the key in the DSS; therefore, the DSS must be turned to the unrestricted UDD and the key removed after each use by a trusted user. If a user has not been assigned a key, the user is a general user.

Administrator
A member of a customer organization who is trusted by the customer organization and who has been given the authority to replace hardware components within the TOE. This person is given the Cabinet Key to provide entry into the TOE. An administrator only acts in the administrative role upon using the Cabinet Key and entering the TOE Cabinet. The person who is an administrator may also be a trusted user if that person has in their possession a DSS Key.

[2] For the nic card, power is removed from the processor on the card. Voltage is still supplied to the card from the motherboard

Installer
A person who builds a SuperNet 2000 EAL4/r1 at EESI facilities from components as well as a person who may install the SuperNet 2000 EAL4/r1 at a customer site. An installer only can modify the SuperNet 2000 EAL4/r1 by first taking it out of operation, either at a customer site or at the EESI facilities. Installers have access to all Cabinet Keys. Once a TOE is installed at a customer facility, installers do not have DSS keys.

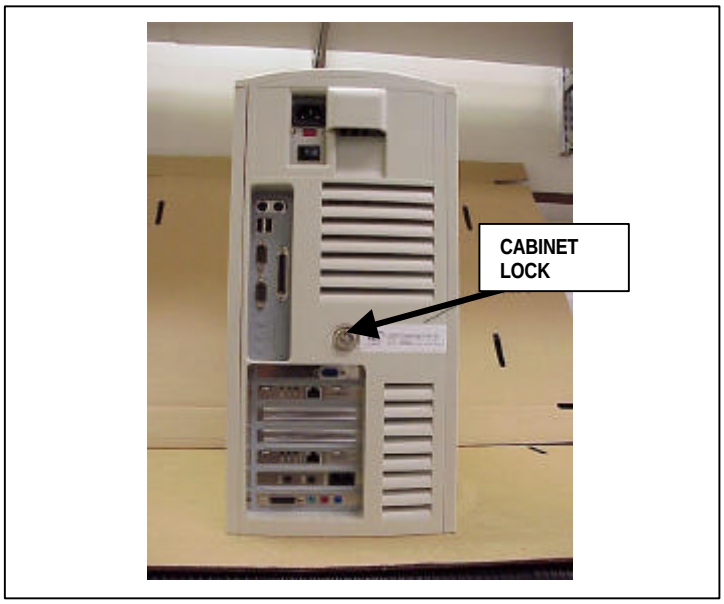

Figure 3 - TOE Back Panel and Cabinet Lock

Network Interface
A network interface to one UDD is the availability of one Network Interface Card (nic) configured and operational in one UDD. The TOE has two nics. Only one has electrical power at a time. The nic not in use has no power to its processor. Throughout this ST, a statement that a specific nic is not operational because it has no electrical power refers to the fact that the processor on the nic has no power and the processor on the nic is not operational.

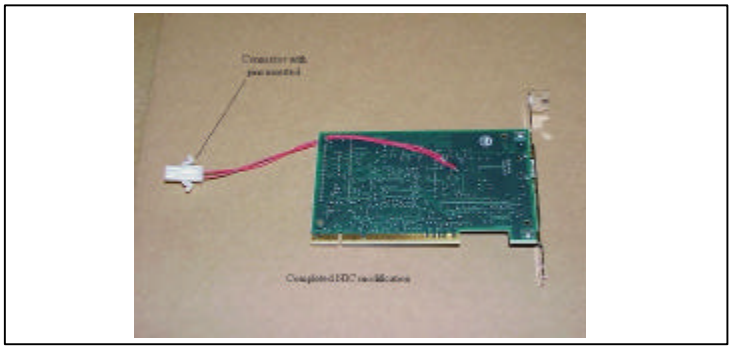

Figure 4 - TOE Network Interface Card with Power Modification

2.2.2 Acronyms

The following abbreviations from the Common Criteria are used in this Security Target:

- CC - Common Criteria for Information Technology Security Evaluation
- EAL - Evaluation Assurance Level
- IT - Information Technology
- PP - Protection Profile

- SFP - Security Function Policy
- ST - Security Target
- TOE - Target of Evaluation
- TSC - TSF Scope of Control
- TSF - TOE Security Functions
- TSP - TOE Security Policy

2.3 Document Organization

This section provides a brief outline of the ST.

1. Section 1 provides a revision history to track the changes made to the Security Taerget.
2. Section 2 provides the introductory material for the ST.
3. Section 3 provides general purpose and TOE description.
4. Section 4 provides a discussion of the expected environment for the TOE. This section also defines the set of threats that are to be addressed by either the technical counter-measures implemented in the TOE hardware or software or through the environmental controls.
5. Section 5 defines the security objectives for both the TOE and the TOE environment.
6. Section 6 contains the functional and assurance requirements derived from the CC, Part 2 and 3, respectively, that must be satisfied by the TOE.
7. Section 7 describes security functions, assurance measures, and assurance evidence.
8. Section 8 provides a rationale to explicitly demonstrate that the information technology security objectives satisfy the policies and threats. Arguments are provided for the coverage of each policy and threat. The section then explains how the set of requirements are complete relative to the objectives, and that each security objective is addressed by one or more component requirements. Arguments are provided for the coverage of each objective. Next Section 8 provides a set of arguments that address dependency analysis, strength of function issues, and the internal consistency and mutual supportiveness of the security target requirements

2.4 Target of Evaluation Overview

This ST describes a Target of Evaluation (TOE), that is part of the SuperNet 2000 EAL4/r1 that is an Intel Pentium III workstation, with multiple separate hardware domains within the same workstation. Multiple separate hardware domains are provided with hardware that can only be used in one UDD. The ability to restrict hardware to one domain and to select a specific hardware domain is provided by the presence of a physical switch.

The TOE is composed of the components of the SuperNet 2000 EAL4/r1 workstation and the supporting documents, configuration management system, tests, and procedures necessary to support the TOE Security Functions (TSF). The TOE includes the Domain Selection Switch (DSS), the specially constructed cabinet, and electrical connections between the hardware switch and the following devices:

- Motherboard (electrical connections)
- Hard drive,
- Removable hard drive,
- Floppy Drive, and
- Network Interface Cards.

An electrical connection to control the electrical power to UDD specific devices is required to provide separate UDDs. The TOE is constructed so the motherboard “reset” is activated when switching from one UDD to another. Although not required to satisfy the SFP, the motherboard reset does cause the workstation to reboot whatever operating system is resident for the selected UDD.

2.5 Protection Profile Claims (ASE_PPC)

No known Protection Profile identifies the security features provided by the SuperNet 2000 EAL4/r1 at the time this ST is written.

3 TARGET OF EVALUATION DESCRIPTION (ASE_DES)

This section provides a physical TOE description, a TSF logical decomposition, a TOE architectural model, and a set of TOE security features.

3.1 Physical TOE Description

The TOE is composed of components of the SuperNet 2000 EAL4/r1 workstation and supporting guidance documentation for users and administrators. The TOE includes

- Tamperproof Cabinet Case,
- Cabinet Lock,
- Domain Selector Switch (DSS)
- DSS Lock
- EES Power Pack
- Motherboard: SuperMicro SUPER P6DBE
- Hard Drives:
  - 10.1GB ATA (Internal)
  - 10.1GB ATA (Removable)
- 5-1/2-inch Removable Hard Drive Case
- Floppy Drive: 3.5-inch Dual 1.44/LS-120MB
- Network Interface Card (NIC): 3Com Etherlink XL
- Cables
- User and Administration Documentation

An electrical connection to control the electrical power to certain devices is required to provide separate UDDs. The electrical connection to the motherboard provides a connection between the DSS and the motherboard "reset, so that the workstation reboots after a UDD is selected.

TOE provides the following functionality

- Ability to use a single computer workstation to securely access two separated UDDs by using a hardware Domain Selection Switch (DSS) to control electrical power to a specific UDD,
- Separate all information (user data, system data, applications, and operating system) that resides on a hard drive to a single UDD,
- Restrict access to sensitive information resigning on one hard drive,
- Restrict access to a floppy drive to only one UDD,
- Provide physically separate operating environments that contain network interfaces,
- Prevent programs on one connected network to use the TOE as a gateway into another network.

The TOE is not expected to:

- Provide complete information flow protection from one operating domain to another, since certain devices are active when either UDD is active (e.g. motherboard, keyboard, mouse, monitor)
- Provide security features and controls (e.g., operating system, file access controls) necessary for a user to interact with a specific operating environment.

3.2 TOE Architecture Model

Figure 5 - TOE Architectural Model describes the TOE architectural model. The TOE provides an access control security policy that restricts access to one of two hardware domains within a single workstation. Each hardware domain is selected using a mechanical switch. Access to the restricted domain is controlled through a physical lock and controlled access to the physical key that operates the lock. Individuals without access to the restricted domain are not given the key. The unrestricted hardware domain may be accessed by any user within an environment where every user can be expected not to attempt to violate the written instructions they are given.

The TSF enforces the access control policy by providing electrical power to specific hardware in one domain at a time. The hardware controlled are the devices that can permanently store user data.

Furthermore access to hardware electrical connections to the physical switch are restricted to administrators. This access is controlled through a specially constructed cabinet with a physical lock. Only administrators are given the key to unlock the Cabinet Lock.

Security Policies
The SuperNet 2000 EAL4/r1 has four security policies.

1. The TSP restricts a user to operate a SuperNet 2000 EAL4/r1 workstation in only one UDD at a given time [Single UDD Policy]
2. Only a trusted user in possession of a DSS key can select either UDD (public and restricted), and thus access to the restricted UDD is controlled by the DSS key [Restricted UDD policy],
3. No executing entity communicating from a connected network to the TOE when in one UDD can communicate to the network connected to the other UDD. This policy is a refinement of the Single UDD policy since each UDD can only have one network connection. Since the Single UDD security policy only allows one active UDD at a given time, two network connections can never be operational at the same time.
4. Only authorized individuals can access the TOE internal interfaces [Authorized Access].

Subject
There are two subjects, one trusted, and one administrative. The trusted subject is the action of turning the DSS from one domain to another. The only way to create a subject is for a user to be in possession of a DSS Key that provides access to the restricted UDD. This is true because a user with access to the physical key only inserts the key to switch the DSS to the restricted domain. The same user is instructed, in writing, to never physically leave the TOE with the DSS Key still in the DSS Lock. The only way to remove the DSS Key is to return the DSS to the unrestricted UDD. Therefore, every time any person physically approaches the TOE the DSS is selecting the unrestricted UDD and no key is necessary to use this UDD. Since the subject under the control of the TOE is the action of turning the DSS, and only users with the DSS Key can turn the DSS, the action performed necessary to create a subject (e.g. turning the DSS) is restricted to users with a DSS Key who are considered trusted.

Users who have no DSS Key cannot create a subject under the control of the TOE. These users can access hardware in the public UDD.

The administrative subject is the action of turning the Cabinet Lock to enter the internal electrical connections of the cabinet. Only administrators and installers, which are trusted roles, have access to the Cabinet Key.

Objects
Objects are hardware devices that permanently store user data and are connected to the DSS.

Security Attributes
All devices in the TOE are categorized by two security attributes: external electrical power, and sharing. A hardware device has external electrical power when sufficient voltage can be measured on an external interface designed to provide power to the device. No external electrical power can be measured to a device unless the DSS is selecting a UDD in which the device resides. When a device is receiving electrical power the device is considered "**active**."

Some devices are active in a single UDD (e.g., hard drive, floppy, and nic). These devices can only receive electrical power when one specific UDD is selected and are considered "**non-shared**" devices. Other devices are active when either UDD is selected. These devices (e.g., motherboard) receive electrical power when either UDD is selected. A device that is active in both the Public and Restricted UDDs is said to be a "**shared**" device. No shared device is an object.

The following table identifies all possible device states relative to the two security attributes; electrical power and sharing, and the hardware that belong to a particular state is identified.

Table 1 - DSS Position and Devices Connected

DSS POSITION/ DEVICES	SHARED DEVICES	OBJECTS - NON-SHARED DEVICES
UDD - Public	Motherboard, video card, sound card, CD-ROM drive, speakers, monitor, mouse, keyboard	Network Interface Card (nic)[Public], fixed hard drive, floppy drive
UDD - Restricted	Motherboard, video card, sound card, CD-ROM drive, speakers, monitor, Mouse, keyboard	Removable hard drive, nic [Sensitive]

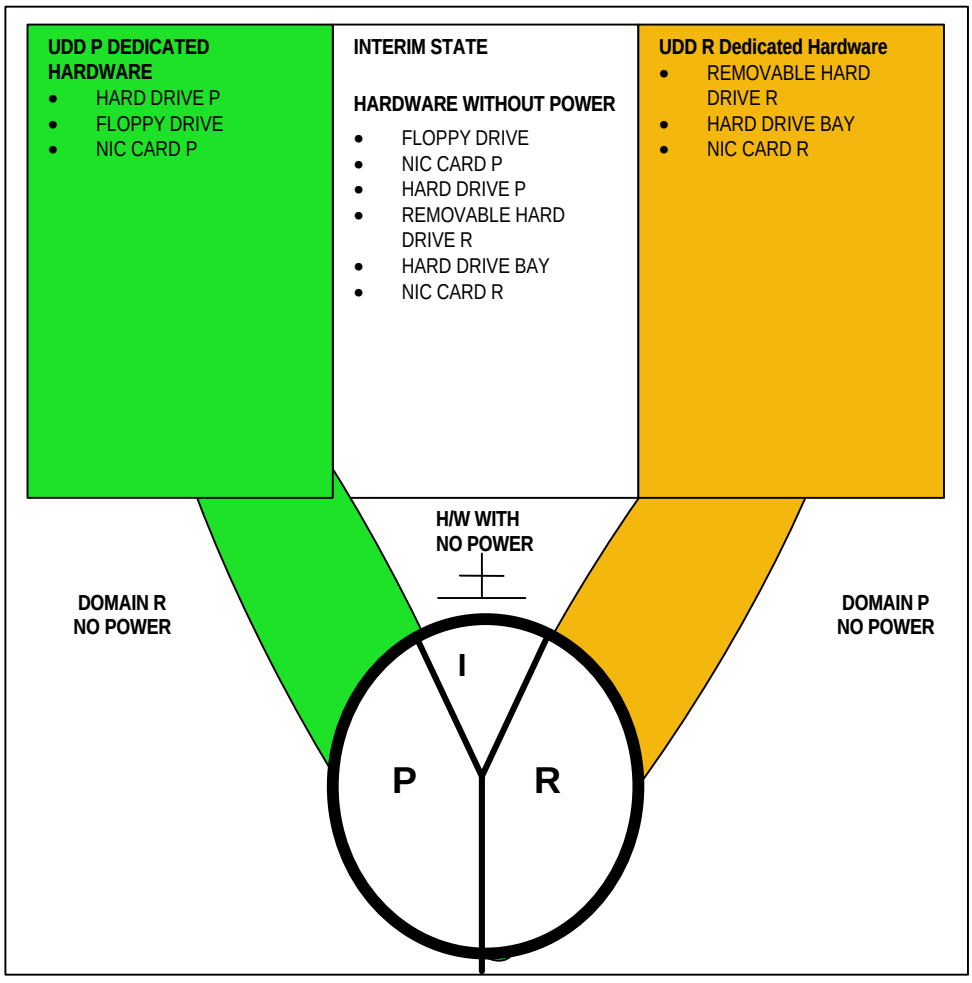

Figure 5 - TOE Architectural Model

3.3 Logical Scope and Boundary

The TOE provides the following security features:

3.3.1 User data protection

The TOE includes hardware devices that store user data. Access is controlled to these devices by removing electrical power from devices that are not associated with the selected UDD, therefore rendering data stored on these devices unavailable.

Two UDDs are identified. One UDD is available to any user with physical access to the TOE. This UDD is designed to provide public or non-sensitive data. The other UDD requires an Identification and Authentication to select. This UDD is designed to provide access to restricted information and the selection of this UDD is restricted to one user and an administrator.

3.3.2 Access control mechanism

Access to the Public UDD is afforded to any person who has physical access to the TOE. Access to the restricted UDD is limited to the user who has in their possession a physical key (DSS Key) that must be inserted into the DSS to turn the switch to provide electrical power to devices connected in the Restricted UDD. All users who are assigned a DSS Key are instructed never to leave the key in the DSS when the TOE is inactive. DSS keys can be removed from the DSS only after the DSS is switched to the Public UDD. Therefore, whenever a user physically approaches the TOE workstation, the DSS is always selecting the Public UDD and no electrical power is provided to devices that are limited to the Restricted UDD.

3.3.3 Identification and Authentication

Users who have access to public information require no identification other than they have been granted physical access to the TOE in an environment where access is restricted to those who can be trusted to follow instructions in the user guide. Users who have access to restricted information are identified by their unique token, the DSS Key. Each DSS key has a serial number. The Administrator Guide informs the customer that when the DSS Key is assigned to an individual, the site administrator is instructed to record the user name and the DSS Key serial number, so that a specific user can be associated with a DSS Key.

The authentication device is the DSS Lock and DSS Key pair. A pair of DSS Keys fit one lock and both keys in the pair have the same serial number as the lock. There are 26**6 possible numbers. There are 14,000 possible key configurations. Only a DSS Key that matches the DSS Lock can be inserted into the specific DSS. When the DSS Key is inserted into the DSS Lock, the DSS can be turned to access devices with sensitive information. DSS Locks and Keys are serial-numbered as pairs.

3.3.4 Security Management

Physical access to the TOE is controlled by the customer. Access to the TOE must be restricted to individuals who will abide by the assumptions identified in the ST. Within these constraints, the TOE security features are managed through the enforcement of roles and keys.

3.3.4.1 Keys

Each DSS has two identical keys with identical serial numbers that are the same as the serial number for the DSS lock. One DSS key is assigned to the trusted user for each workstation. The other DSS key is assigned to an administrator. An administrator may control many DSS keys. A trusted user may have only one DSS key at any given time.

The Cabinet Key operates the Cabinet Lock on the back panel of the workstation. Each Cabinet Lock has two Cabinet Keys that are serial-numbered to the Cabinet Lock. Each TOE is shipped with one Cabinet Key and EESI maintains one Cabinet Key in their possession.

A discussion of key management is included in the User Guidance document shipped with each TOE. The management of Cabinet Keys by EESI includes sufficient information to cross-reference a specific instantation of the TOE to a specific Cabinet Key. EESI maintains secure storage for all Cabinet Keys as well as a database of Cabinet Key numbers, customer name and location, and workstation identification and location information.

3.3.4.2 Roles

The TOE supports four roles; "general user," "trusted user," "administrator" and "installer." Each role is described below:

- General user - individual that has physical access to the operating TOE and has not been assigned any physical keys associated with the TOE.
- Trusted user - user who has in their possession a DSS Key, and not a Cabinet Key, and is, therefore, provided access to the Restricted UDD,
- Administrator - person with a DSS Key and a Cabinet Key for a specific copy of the TOE. An administrator has access to all DSS Keys and Cabinet Keys for each copy of the TOE purchased by the customer for which the administrator has been granted specific access by the customer. An administrator has complete access to all TOE devices.
- Installer - individual authorized by EESI who is in possession of the Cabinet and DSS Keys for one copy of the TOE and who has access to all Cabinet Keys for every copy of the TOE ever built. Cabinet Keys are made in pairs. EESI sends one Cabinet Key with every copy of the TOE shipped, and EESI retains one Cabinet Key. When installing the TOE at a customer's location, the installer uses the Cabinet Key shipped with the TOE. The installer has access to the EESI held Cabinet Key for every product shipped in case the customer's Cabinet Key can not be found and there is a system problem that EESI is responsible for repairing. An installer can modify the TOE.

3.3.5 Protection of the TSF

The TSF protects itself from tampering, by protecting the electrical connections between the DSS and UDD hardware devices. To do this, the TOE employs a specially constructed case. The shell of the case interlocks such that unless forced entry is employed that provides visible evidence, the back of the case must be removed first. The back of the case is secured with a lock similar to the DSS Lock. Only EESI authorized installers and customer administrators have access to the Cabinet Key, so only individuals in these trusted roles can maintain the electrical configuration of the TOE. This restricted access to physical connections between the DSS and TOE hardware devices ensures that the DSS electrical connections to TOE hardware devices are appropriate to separate UDDs correctly.

Users are instructed to perform a visual inspection of the cabinet for signs of forced entry before using the workstation. If signs of forced entry are evident, users are instructed to immediately contact their security officer and not to attempt to use the workstation. Additionally, users are instructed not to modify any of the cable connections to the TOE cabinet, and not to substitute or modify any peripheral devices.

4 SECURITY ENVIRONMENT (ASE_ENV)

This chapter identifies

- Significant assumptions about the TOE's operational environment,
- IT related threats to the organization countered by the TOE, and
- Environmental threats requiring controls to provide sufficient protection.

4.1 Secure Usage Assumptions

The specific conditions listed below are assumed to exist in the TOE environment. These assumptions include both practical realities in the implementation of the TOE security requirements and the essential environmental conditions on the use of the TOE.

Table 2 - Secure Usage Assumptions

TYPE	NAME (A = ASSUMPTION)	ASSUMPTION	DISCUSSION
Physical	A.PHYSICAL	The TOE is physically secure.	Physical tampering of the TOE is prevented.
Physical	A.KEYS	Access to keys is restricted. When physical access to keys is granted, this action is considering granting access to the part of the TOE protected by the lock that is serial-numbered paired to a key.	Both the DSS and the physical cabinet have locks that required physical keys to access and keys are specific to locks. Locks are of a high security design with keys legally impossible to duplicate and locks construction that provides a significant number of unique keys.
Personnel	A.ADMIN	Only a person who has in their possession the Cabinet Key can modify the TSF.	Only installers and administrators can perform administrative functions for the TOE.
Personnel	A.MODIFY	Modifications to the TOE are performed by competent authorized individuals with physical access to internal hardware.	Installers and administrators receive training using materials provided by EESI.
Personnel	A.NOEVIL	Authorized administrators and installers are non-hostile.	Administrators and installers follow all administrator guidance; however, they are capable of error.
Personnel	A.SECURITY-AWARE	Users recognize the need for a secure IT environment and follow all usage guidance.	It is essential that the users appreciate the need for security.
Personnel	A.TRUSTED	Any user with a DSS key in their possession is a trusted user with access to restricted information	Users are instructed not to share the DSS Key with another user and never to leave the key in the DSS when they are no longer using the TOE.

4.2 Threats to Security

The security threats facing the TOE are listed in Table 3 - Security Threats and the threats to the surrounding environment are listed in Table 4 - Security Threats Addressed by the TOE Operating Environment.

Table 3 - Security Threats

NAME (T = THREAT)	THREAT
T.CABINET_COMPROMISE	The Cabinet Lock could be opened by a key other than the Cabinet Key paired to the lock.
T.CONFIGURATION	The TOE user, or an individual on one of the network connections, could modify TOE configuration settings.
T.DSS_COMPROMISE	The DSS lock can be operated with a key other than the DSS Key paired to the lock.
T.NETWORK_ISOLATE	A program executed on one connected network could use the TOE as a gateway to communicate with the other connected network.
T.SENSITIVE	A user who has not been granted access to sensitive information may access it if the user has physical access to the TOE.
T.SPOOF	Via intentional or unintentional actions, a user may think the non-shared peripherals are connected to a selected domain when indeed they are connected to the other.
T.SWITCH_FAILURE	The DSS fails to correctly select UDD hardware.

Table 4 - Security Threats Addressed by the TOE Operating Environment

NAME (T = THREAT, E = ENVIRONMENT)	THREAT
T.E.ADMIN	The TOE may be incorrectly administered in a manner that undermines security.
T.E.PHYSICAL	Security-critical parts of the TOE may be subjected to a physical attack that may compromise security.

5 SECURITY OBJECTIVES (ASE_OBJ)

This section defines the security objectives of the TOE and its supporting environment. Security objectives, categorized as either TOE security objectives or environment security objectives, reflect the stated intent to counter identified threats and/or comply with any organizational security policies identified. All of the identified threats, assumptions, and organizational policies are addressed under one of the categories below.

5.1 TOE Security Objectives

The following are the TOE's IT security objectives:

Table 5 - TOE Security Objectives

OBJECTIVE	DESCRIPTION
O.BYPASS	Users can only select the UDD by manually using the DSS.
O.CONFIGURATION	The TOE will protect configuration settings (DSS connections) from being altered by any individual other than the Installer or the Administrator.
O.DETECT	Unauthorized physical entry into the TOE cabinet shall be detectable by a user.
O.FLOPPY	The TOE will prevent the availability of a floppy in the transition state and in one of the two hardware environments.
O.INDICATE	A user receives an unambiguous indication of which UDD has been selected.
O.ISOLATE	TOE shall isolate user information on the hard disk, removable media and network interfaces to a single UDD.
O.MODIFY	Only an EESI designated installer or a customer-designated administrator may install, modify and repair connections inside the TOE case. These connections are between the DSS and specific hardware devices.
O.RESTRICTED_ACCESS	Access to the restricted UDD is limited to users in possession of the physical DSS key that is paired to the specific DSS.
O.SELECT	An explicit action by the user is used to select the UDD to which the shared set of devices is connected.

5.2 Environmental Security Objectives

Certain objectives with respect to the general operating environment must be met. The following are the TOE's environmental security objectives.

Table 6 - Environmental Security Objectives

OBJECTIVE	DESCRIPTION	ASSUMPTIONS
O.E.ENVIRON	The TOE environment must be appropriate to facilitate proper operation and maintenance and it must be maintained in accordance with this objective.	A.ADMIN A.MODIFY, A.PHYSICAL, A.SECURITY-AWARE T.E.PHYSICAL
O.INSTALL	Those responsible for the TOE must ensure that the TOE is installed, managed, and operated in a manner which maintains IT security.	A.ADMIN A.NOEVIL T.E.ADMIN
O.E.MANUAL.LOG	A manual record is maintained by a customer security officer that identifies which users have been assigned a DSS Key and/or a Cabinet Key	A.KEYS T.CONFIGURATION T.SENSITIVE
O.E.PHYSICAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from physical attack that might compromise IT security.	T.E.PHYSICAL, A.ADMIN A.PHYSICAL A.TRUSTED

6 IT SECURITY REQUIREMENTS (ASE_REQ)

This section defines the detailed IT security requirements that are satisfied by the TOE or its environment. TOE security requirements shall be stated as follows:

1. **TOE security functional requirements (SFRS)** are defined as functional components drawn from Part 2 where applicable. The TOE meets all the SFRS claimed in the next section.
2. **TOE security assurance requirements (SARS)** are defined as the assurance components drawn from Part 3 of the CC where applicable. The TOE meets all SARS required for EAL4.
3. The optional statement of **security requirements for the IT environment** identifies the IT security requirements that are to be met by the IT environment of the TOE.

   These requirements are discussed in separate sub-sections within this section. For specific requirements, there are no refinements or iterations included in the ST.

6.1 TOE Security Functional Requirements (SFRs)

The CC divides security requirements into two categories: Security functional requirements (SFRs), and Security assurance requirements (SARs). SFRs describe requirements for security functions such as information flow control, audit, identification and authentication, while SARs **provide** grounds for confidence that the TOE meets its security objectives (for example, configuration management, testing, vulnerability assessment).

Table 7 - Functional Components lists the IT functional requirements and the security objectives each requirement helps to address. All functional and assurance dependencies associated with the components in Table 8 have been satisfied.

Table 7 - Functional Components

CC COMPONENT	NAME	HIERARCHICAL TO	DEPENDENCY	OBJECTIVES FUNCTION HELPS ADDRESS
FDP_ACC.1(a) FDP_ACC.1(b) FDP_ACC.1(c)	Subset access control	None	FDP_ACF.1	O.CONFIGURATION
FDP_ACF.1(a) FDP_ACF.1(b) FDP_ACF.1(c)	Security attribute based access control	None	FDP_ACC.1 FDP_MSA.3	O.CONFIGURATION O.MODIFY O.RESTRICTED_ACCESS
FIA_UAU.1	Timing of authentication	Non	FIA_UID.1	O.MODIFY O.RESTRICTED_ACCESS
FIA_UID.1	Timing of identification	None	None	O.CONFIGURATION O.SELECT
FMT_MOF.1	Management of security functions behavior	None	FMT_SMR.1	O.CONFIGURATION
FMT_MSA.1	Management of Security Attributes	None	FDP_ACC.1 FMT_SMR.1	O.CONFIGURATION
FMT_MSA.3	Static attribute initialization	None	FMT_MSA.1 FMT_SMR.1	O.CONFIGURATION
FMT_SMR.1	Security management roles	None	FIA_UID.1	O.E.PHYSICAL
FPT_PHP.1	Passive detection of physical attack	None	FMT_MOF.1	O.DETECT
FPT_RVM.1	Non-Bypassability of the TSF	None	None	O.BYPASS O.CONFIGURATION O.FLOPPY O.ISOLATE O.SELECT
FPT_SEP.1	TSF domain separation	None	None	O.CONF O.INDICATE O.ISOLATE

The functional requirements in the above table are described below in further detail. They are derived verbatim from the Common Criteria Version 2.1 Part 2, with the exception of italicized items listed in

brackets. These bracketed items include either “assignments” that are TOE specific or “selections” from the Common Criteria that the TOE enforces.

6.1.1 User Data Protection (FDP)

6.1.1.1 FDP_ACC.1 Subset access control

Hierarchical to: No other components.

6.1.1.1.1 FDP_ACC.1(a)

FDP_ACC.1.1 The TSF enforces the [assignment: **the Restricted UDD policy]** on [assignment: **trusted users accessing a restricted UDD.**].

6.1.1.1.2 FDP_ACC.1(b)

FDP_ACC.1.1 The TSF enforces the [assignment: **the Authorized Access policy]** on [assignment: **installers and administrators accessing the interfaces and devices internal to the TOE.]**

6.1.1.1.3 FDP_ACC.1(c)

FDP_ACC.1.1The TSF enforces the [assignment: the **Single UDD policy**] on [assignment: **any person operating the TOE.]**

Policy refinement: Since only one UDD at a time can be selected and have electrical power at one time, no executing entity communicating from a connected network to the TOE when in one UDD can communicate to the network connected to the other UDD. This policy is a refinement of the Single UDD policy since each UDD can only have one network connection. Since the Single UDD security policy only allows one active UDD at a given time, two network connects can never be operational at the same time

Dependencies: FDP_ACF.1Security attribute based access control

6.1.1.2 FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.

6.1.1.2.1 FDP_ACF.1.1(a)

FDP_ACF.1.1 The TSF enforces the [assignment**: Restricted UDD policy**] based on [assignment: **possession of a physical key**].

FDP_ACF.1.2. The TSF enforces the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: **if a user has in their possession a DSS key, the user is a trusted user and may access the sensitive UDD**].

FDP_ACF.1.3 The TSF explicitly authorizes access of subjects to objects based on the following additional rules: [assignment**: Access to objects that are the devices controlled by the DSS switch selection is controlled by the physical electrical connection of specific devices to one physical DSS position or UDD. When one physical DSS position is selected access is granted to all devices connected to that switch position and only that switch position.**]

FDP_ACF.1.4: The TSF explicitly denies access of subjects to objects based on the [assignment: **NONE**].

6.1.1.2.2 FDP_ACF.1(b)

FDP_ACF.1.1 The TSF enforces the [assignment**: the Authorized Access security policy**] based on [assignment: **possession of a physical key**].

FDP_ACF.1.2 The TSF enforces the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment **If a user has in their possession the physical key to the TOE cabinet, then the user is an installer or an administrator and can modify the TOE**].

FDP_ACF.1.3 The TSF explicitly authorizes access of subjects to objects based on the following additional rules: [assignment**: Access to objects that are the devices controlled by the DSS switch selection is controlled by the physical electrical connection of specific devices to one physical DSS position or UDD. When one physical DSS position is selected access is granted to all devices connected to that switch position and only that switch position.**]

FDP_ACF.1.4: The TSF explicitly denies access of subjects to objects based on the [assignment: **NONE**].

6.1.1.2.3 FDP_ACF.1(c)

FDP_ACF.1.1 The TSF enforces the [assignment: the **Single UDD policy**] on [assignment: **all subjects].**

FDP_ACF.1.2. The TSF enforces the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: **When a user is in possession of a DSS Key, the DSS can only select one UDD at a time**].

FDP_ACF.1.3 The TSF explicitly authorizes access of subjects to objects based on the following additional rules: [assignment**: Access to objects that are the devices controlled by the DSS switch selection is controlled by the physical electrical connection of specific devices to one physical DSS position or UDD. When one physical DSS position is selected access is granted to all devices connected to that switch position and only that switch position.**]

FDP_ACF.1.4: The TSF explicitly denies access of subjects to objects based on the [assignment: **NONE**].

Rationale: When the term “access” is used, it refers to electrical connectivity such that when the operating system (whatever it is) is initialized or booted, the only devices that can be recognized by the operating system are those that have an electrical connection. The user accessing information on devices through an operating system can only access information on devices that have an electrical connection (receive electrical power

Dependencies: FDP_ACC.1Subset access control, FMT_MSA.3Static attribute initialization

6.1.2 Identification and Authentication (FIA)

6.1.2.1 FIA_UAU.1 Timing of authentication

Hierarchical to: No other components.

FIA_UAU.1.1 The TSF allows [assignment: **access to the Public UDD**] on behalf of the user to be performed before the user is authenticated.

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

Dependencies: FIA_UID.1Timing of identification

Rationale: Access to the Public UDD only requires physical access to the TOE, since the DSS only selects the Public DSS when not in use and a user first approaches the TOE. If a general user has no DSS Key, then the Public UDD is the only domain available for use. (e.g. only the non-shared hardware connected to the Public UDD DSS position is active) A user must be in possession of a physical key to perform any other task on the TOE. Each physical DSS Key is serial-numbered to one DSS and each trusted user receives one DSS Key, so the DSS Key-Lock pair is a unique authentication mechanism to authenticate a trusted user before allowing access to the Restricted UDD.

The authorized access policy restricts access into the cabinet to any administrator or installer who has been assigned a Cabinet Key. Each Cabinet Lock has a Cabinet Key that is a serial numbered to the lock. There is only one Cabinet Key for each workstation available to the administrative role and administered by the customer security officer, and one Cabinet Key maintained by EESI or their assignee that is restricted to the installer role. Therefore access into the TOE Cabinet can be uniquely linked to a specific person and the Cabinet Key-Lock pair is the unique authentication device for the administrative and installer role[3].

6.1.2.2 FIA_UID.1 Timing of identification

Hierarchical to: No other components.
FIA_UID.1.1 The TSF allows [assignment: **access to the Public UDD**] on behalf of the user to be performed before the user is identified.

Rationale: Any user with physical access to the TOE may access the public UDD without first providing identification or authentication.

FIA_UID.1.2: The TSF requires each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: No dependencies.

Rationale: A user must be in possession of a physical key to assume a trusted role (trusted user, administrator, or installer). If a user is in possession of a DSS Key, the user is either a trusted user who has access to the restricted UDD for a specific workstation or the administrator who has access to more than one workstation. If any higher-level abstractions (e.g. network interfaces, files, operating system) have been accessed on the restricted UDD, the administrator can uniquely identify the user who had access to the restricted UDD.

6.1.3 Security Management (FMT)

6.1.3.1 FMT_MOF.1 Management of security functions behavior

Hierarchical to: No other components.

FMT_MOF.1.1: The TSF restricts the ability to [selection: ***determine the behavior of, disable, enable, or modify the behavior of***] the functions [assignment: accessing the inside of the Cabinet, modifying domain attachments to the DSS, changing electrical connections to any hardware device, or replacing a hardware device] to [assignment: an **administrator or an installer**].

Dependencies: FMT_SMR.1 Security roles

[3] Two keys, one a copy of the other, are cut for one DSS Lock and likewise two keys are cut for one Cabinet Lock. Each pair of keys is unique to the specific Lock. Just as a User-id is a unique identifier, it is possible for a key-tumbler pattern to repeat, even though it is highly unlikely. See Strength of TOE Function (AVA_SOF) in the assurance requirement section.

Rationale: There are ten security functions performed by the TSF. All security functions except for two of them are enabled, disabled, or their behavior modified by either an installer or an administrator.[4] Both of these security functions are provided through secure usage assumptions.

An installer and an administrator have the same access rights to each installed TOE for which they have been given the Cabinet Key. However an administrator is always assigned by a customer and access is always limited to installed TOEs that have been purchased by that customer. An installer could be granted access to any copy of the TOE for which EESI retains one Cabinet Key out of the pair of Cabinet Keys. Therefore, unless EESI has delivered, as a specific contract deliverable, both Cabinet Keys to the customer, an installer could access installed TOE copies for more than one customer (e.g., part of a support contract).

6.1.3.2 FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.
FMT_MSA.1.1The TSF enforces the [assignment: **Authorized Access SFP**] to restrict the ability to [selection: **change_default, modify, delete**] the security attributes **[electrical power, sharing] to [installers, administrators].**

Rationale: All devices in the TOE are categorized by two security attributes: external electrical power, and whether a device can be shared by more than one UDD. By controlling the availability of electrical power to non-shared devices (objects), the TSF enforces security policies. Administrators and installers can modify which devices are active when a specific UDD is selected by the DSS. They can modify which device receives electrical power and which devices are objects and which devices are shared between multiple UDDs.

Dependencies: FDP_ACC.1Subset access control, FMT SMR.1 Security roles

6.1.3.3 FMT_MSA.3 Static attribute initialization

Hierarchical to: No other components.

FMT_MSA.3.1The TSF enforces the [assignment: **Restricted UDD SFP**] to provide [**selection*: access to the Restricted UDD through the physical possession of a DSS Key***] default values for security attributes that are used to enforce the *SFP*.

FMT_MSA.3.2The TSF allows the [assignment**: the installer or the administrator**] to specify alternative initial values to override the default values when an object or information is created.

Dependencies: FMT_MSA.1Management of security attributes, FMT_SMR.1Security roles

Rationale: The TOE provides all users default access to the Public UDD selected by the DSS. Only trusted users with a DSS Key may select the Sensitive UDD by first inserting the DSS Key into the DSS.

The installer and the administrator can alter the electrical connections between the DSS and the hardware devices such that the default is the Sensitive UDD and the DSS Key is needed to select the Public UDD.

6.1.3.4 FMT_SMR.1 Security Roles

Hierarchical to: No other components.

FMT_SMR.1.1The TSF maintains the roles [assignment: **of general user, trusted user, administrator, and installer].**

[4] The two security functions that cannot be affected by an installer or an administrator are: 1) DSS keys are restricted and match one DSS, and 2) keys to cabinet locks are restricted to installers and administrators.

FMT_SMR.1.2The TSF is able to associate users with roles.

Dependencies: FIA_UID.1Timing of identification

Rationale: Any person with physical access to the TOE may be a general user, a trusted user, or an installer.
Any person with a key to the DSS may be a trusted user, authorized administrator, or an installer.
Any person with the key to the cabinet is an authorized administrator or an installer.

6.1.4 Protection of the TSF (FPT)

6.1.4.1 FPT_PHP.1 Passive detection of physical attack

Hierarchical to: No other components.

FPT_PHP.1.1 The TSF provides unambiguous detection of physical tampering that might compromise the TSF.

FPT_PHP.1.2 The TSF provides the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.

Dependencies: FMT_MOF.1 Management of security functions behavior

Rationale: The TOE protects itself from tampering, by protecting the electrical connections between the DSS and UDD hardware devices. To do this, the TOE employs a specially constructed case. The shell of the case interlocks such that unless forced entry is employed that provides visible evidence, the back of the case must be removed first. The back of the case is secured with a lock similar to the DSS Lock. Only EESI installers and customer administrators have access to the Cabinet Key, so only individuals in these trusted roles can maintain the electrical configuration of the TOE. This restricted access to physical connections between the DSS and TOE hardware devices ensures that the DSS electrical connections to TOE hardware devices are appropriate to separate UDDs correctly.

Users are instructed to perform a visual inspection of the cabinet for signs of forced entry before using the workstation. If signs of forced entry are evident, users are instructed to immediately contact their security officer and not to attempt to use the workstation.

6.1.4.2 FPT_RVM.1 Non-Bypassability of the TSP

Hierarchical to: No other components.

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

Rationale: General Users and Trusted Users who use the TOE to perform work are separated by the TSF from individuals who modify and maintain the TOE, installers and administrators. General and trusted users cannot modify the TSF. This activity is reserved for installers and administrators. For "users," there is only one visible function and that function is controlled by the TSF. This single external interface is switching from one UDD to another UDD by turning the DSS. A key feature for ensuring the TSP enforcement functions are invoked is the "interim" state that all operating domain transitions must go through.

All objects (devices with the non-sharable security attribute) only receive electrical power when the DSS selects their associated UDD. Electrical power to all objects is removed when the DSS goes thought the "interim" state when transitioning from one UDD to another UDD.

The TSP enforcement functions are hardwired to a physical switch. Upon selecting the other UDD, through the use of the DSS, the TSP enforcement functions are always invoked before any activity can occur in that domain.

Dependencies: No dependencies.

6.1.4.3 FPT_SEP.1 TSF domain separation

Hierarchical to: No other components.

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

Rationale: The DSS is the TOE interface that implements the SFP. The DSS is protected from modification. Connections between the DSS and the objects it controls also are protected from modification.

FPT_SEP.1.2 The TSF enforces separation between the security domains of subjects in the TSC. Dependencies: No dependencies.

Rationale: The security domain for a user is a specific UDD. The TOE separates these domains for all objects controlled by the TOE. The context switching controlled by the DSS restricts a user to a specific UDD.

Dependencies: No dependencies.

6.2 Security Assurance Requirements (SARs)

This section outlines the assurance requirement components in this Security Target that were drawn from Part 3 of the Common Criteria necessary to meet the EAL 4 level of assurance. Following the outline, a description of each assurance identified in the outline is included from the Common Criteria for the EAL 4 level of assurance.

Table 8 - Meeting EAL4 Assurance Requirements identifies the EAL 4 assurance requirements and the assurance class. All assurance dependencies associated with the components in Table 9 have been satisfied. The assurance classes and assurance components for the TOE, and the evidence identified that meets the assurance requirements are provided in Table 15 - Assurance Classes Satisfied.

Table 8 - Meeting EAL4 Assurance Requirements

ASSURANCE CLASS	ASSURANCE COMPONENTS
Configuration Management	ACM_AUT.1 Partial CM automation
	ACM_CAP.4 Generation support and acceptance procedures
	ACM_SCP.2 Problem tracking CM coverage
Delivery and Operation	ADO_DEL.2 Detection of modification
	ADO_IGS.1 Installation, generation, and start-up procedures
Development	ADV_FSP.2 Fully defined external interfaces
	ADV_HLD.2 Security-enforcing high-level design
	ADV_IMP.1 Subset of Implementation of the TSF
	ADV_LLD.1 Descriptive low-level design
	ADV_RCR.1 Informal Correspondence demonstration
	ADV_SPM.1 Informal TOE security policy model
Guidance Documents	AGD_ADM.1 Administrator guidance
	AGD_USR.1 User guidance
Life Cycle Support	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.1 Well-defined development tools
Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: high-level design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
Vulnerability Assessment	AVA_MSU.2 Validation of analysis
	AVA_SOF.1 Strength of TOE security function evaluation
	AVA_VLA.2 Independent vulnerability analysis

6.2.1 TOE Assurances Described

ACM_AUT.1 Partial CM automation

Developer action elements:

ACM_AUT.1.1D The developer shall use a CM system.

ACM_AUT.1.2D The developer shall provide a CM plan.

Content and presentation of evidence elements:

ACM_AUT.1.1C The CM system shall provide an automated means by which only authorized changes are made to the TOE implementation representation.

ACM_AUT.1.2C The CM system shall provide an automated means to support the generation of the TOE.

ACM_AUT.1.3C The CM plan shall describe the automated tools used in the CM system.

ACM_AUT.1.4C The CM plan shall describe how the automated tools are used in the CM system.

Evaluator action elements:

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

ACM_CAP.4 Generation support and acceptance procedures

Developer action elements:

ACM_CAP.4.1D The developer shall provide a reference for the TOE.

ACM_CAP.4.2D The developer shall use a CM system.

ACM_CAP.4.3D The developer shall provide CM documentation.

Content and presentation of evidence elements:

ACM_CAP.4.1C The reference for the TOE shall be unique to each version of the TOE.

ACM_CAP.4.2C The TOE shall be labeled with its reference.

ACM_CAP.4.3C The CM documentation shall include a configuration list, a CM plan, and an acceptance plan.

ACM_CAP.4.4C The configuration list shall describe the configuration items that comprise the TOE.

ACM_CAP.4.5C The CM documentation shall describe the method used to uniquely identify the configuration items.

ACM_CAP.4.6C The CM system shall uniquely identify all configuration items.

ACM_CAP.4.7C The CM plan shall describe how the CM system is used.

ACM_CAP.4.8C The evidence shall demonstrate that the CM system is operating in accordance with
the CM plan.

ACM_CAP.4.9C The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.

ACM_CAP.4.10C The CM system shall provide measures such that only authorized changes are made to the configuration items.

ACM_CAP.4.11C The CM system shall support the generation of the TOE.

ACM_CAP.4.12C The acceptance plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.

Evaluator action elements:

ACM_CAP.4.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ACM_SCP.2 Problem tracking CM coverage

Developer action elements:

ACM_SCP.2.1D The developer shall provide CM documentation.

Content and presentation of evidence elements:

ACM_SCP.2.1C The CM documentation shall show that the CM system, as a minimum, tracks the following: the TOE implementation representation, design documentation, test documentation, user documentation, administrator documentation, CM documentation, and security flaws.

ACM_SCP.2.2C The CM documentation shall describe how configuration items are tracked by the CM system.

Evaluator action elements:

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

ADO_DEL.2 Detection of modification

Developer action elements:

ADO_DEL.2.1D The developer shall document procedures for delivery of the TOE or parts of it to the user.

ADO_DEL.2.2D The developer shall use the delivery procedures.

Content and presentation of evidence elements:

ADO_DEL.2.1C 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.2.2C The delivery documentation shall describe how the various procedures and technical measures provide for the detection of modifications, or any discrepancy between the developer's master copy and the version received at the user site.

ADO_DEL.2.3C The delivery documentation shall describe how the various procedures allow detection of attempts to masquerade as the developer, even in cases in which the developer has sent nothing to the user's site.

Evaluator action elements:

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

ADO_IGS.1 Installation, generation, and start-up procedures

Developer action elements:

ADO_IGS.1.1D The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

Content and presentation of evidence elements:

ADO_IGS.1.1C The documentation shall describe the steps necessary for secure installation, generation, and start-up of the TOE.

Evaluator action elements:

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.

ADV_FSP.2 Fully defined external interfaces

Developer action elements:

ADV_FSP.2.1D The developer shall provide a functional specification.

Content and presentation of evidence elements:

ADV_FSP.2.1C The functional specification shall describe the TSF and its external interfaces using an informal style.
ADV_FSP.2.2C The functional specification shall be internally consistent.

ADV_FSP.2.3C The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing complete details of all effects, exceptions and error messages.

ADV_FSP.2.4C The functional specification shall completely represent the TSF.

ADV_FSP.2.5C The functional specification shall include rationale that the TSF is completely represented.

Evaluator action elements:

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

ADV_FSP.2.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

ADV_HLD.2 Security enforcing high-level design

Developer action elements:

ADV_HLD.2.1D The developer shall provide the high-level design of the TSF.

Content and presentation of evidence elements:

ADV_HLD.2.1C The presentation of the high-level design shall be informal.

ADV_HLD.2.2C The high-level design shall be internally consistent.

ADV_HLD.2.3C The high-level design shall describe the structure of the TSF in terms of subsystems.

ADV_HLD.2.4C The high-level design shall describe the security functionality provided by each subsystem of the TSF.

ADV_HLD.2.5C The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

ADV_HLD.2.6C The high-level design shall identify all interfaces to the subsystems of the TSF.

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

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

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

Evaluator action elements:

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

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

ADV_IMP.1 Subset of the implementation of the TSF

Developer action elements:

ADV_IMP.1.1D The developer shall provide the implementation representation for a selected subset of the TSF.

Content and presentation of evidence elements:

ADV_IMP.1.1C The implementation representation shall unambiguously define the TSF to a level of detail such that the TSF can be generated without further design decisions.

ADV_IMP.1.2C The implementation representation shall be internally consistent.

Evaluator action elements:

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

ADV_IMP.1.2E The evaluator shall determine that the least abstract TSF representation provided is an accurate and complete instantiation of the TOE security functional requirements.

ADV_LLD.1 Descriptive low-level design

Developer action elements:

ADV_LLD.1.1D The developer shall provide the low-level design of the TSF.

Content and presentation of evidence elements:

ADV_LLD.1.1C The presentation of the low-level design shall be informal.

ADV_LLD.1.2C The low-level design shall be internally consistent.

ADV_LLD.1.3C The low-level design shall describe the TSF in terms of modules.

ADV_LLD.1.4C The low-level design shall describe the purpose of each module.

ADV_LLD.1.5C The low-level design shall define the interrelationships between the modules in terms of provided security functionality and dependencies on other modules.

ADV_LLD.1.6C The low-level design shall describe how each TSP-enforcing function is provided.

ADV_LLD.1.7C The low-level design shall identify all interfaces to the modules of the TSF.

ADV_LLD.1.8C The low-level design shall identify which of the interfaces to the modules of the TSF are externally visible.

ADV_LLD.1.9C The low-level design shall describe the purpose and method of use of all interfaces to the modules of the TSF, providing details of effects, exceptions and error messages, as appropriate.

ADV_LLD.1.10C The low-level design shall describe the separation of the TOE into TSP-enforcing and other modules.

Evaluator action elements:

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

ADV_LLD.1.2E The evaluator shall determine that the low-level design is an accurate and complete instantiation of the TOE security functional requirements.

ADV_RCR.1 Informal correspondence demonstration

Developer action elements:

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

Content and presentation of evidence elements:

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.

Evaluator action elements:

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

ADV_SPM.1 Informal TOE security policy model

Developer action elements:

ADV_SPM.1.1D The developer shall provide a TSP model.

ADV_SPM.1.2D The developer shall demonstrate correspondence between the functional specification and the TSP model.

Content and presentation of evidence elements:

ADV_SPM.1.1C The TSP model shall be informal.

ADV_SPM.1.2C The TSP model shall describe the rules and characteristics of all policies of the TSP that can be modeled.

ADV_SPM.1.3C The TSP model shall include a rationale that demonstrates that it is consistent and complete with respect to all policies of the TSP that can be modeled.

ADV_SPM.1.4C The demonstration of correspondence between the TSP model and the functional specification shall show that all of the security functions in the functional specification are consistent and complete with respect to the TSP model.

Evaluator action elements:

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

AGD_ADM.1 Administrator guidance

Dependencies:

ADV_FSP.1 Informal functional specification

Developer action elements:

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

Content and presentation of evidence elements:

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.

Evaluator action elements:

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

AGD_USR.1 User guidance

Dependencies:

ADV_FSP.1 Informal functional specification

Developer action elements:

AGD_USR.1.1D The developer shall provide user guidance.

Content and presentation of evidence elements:

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.

Evaluator action elements:

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

ALC_DVS.1 Identification of security measures

Developer action elements:

ALC_DVS.1.1D The developer shall produce development security documentation.

Content and presentation of evidence elements:

ALC_DVS.1.1C The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

ALC_DVS.1.2C The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.

Evaluator action elements:

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

ALC_DVS.1.2E The evaluator shall confirm that the security measures are being applied.

ALC_LCD.1 Developer defined life-cycle model

Developer action elements:

ALC_LCD.1.1D The developer shall establish a life-cycle model to be used in the development and maintenance of the TOE.

ALC_LCD.1.2D The developer shall provide life-cycle definition documentation.

Content and presentation of evidence elements:

ALC_LCD.1.1C The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.

ALC_LCD.1.2C The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.

Evaluator action elements:

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

ALC_TAT.1 Well-defined development tools

Developer action elements:

ALC_TAT.1.1D The developer shall identify the development tools being used for the TOE.

ALC_TAT.1.2D The developer shall document the selected implementation-dependent options of the development tools.

Content and presentation of evidence elements:

ALC_TAT.1.1C All development tools used for implementation shall be well defined.

ALC_TAT.1.2C The documentation of the development tools shall unambiguously define the meaning of all statements used in the implementation.

ALC_TAT.1.3C The documentation of the development tools shall unambiguously define the meaning of all implementation-dependent options.

Evaluator action elements:

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

ATE_COV.2 Analysis of coverage

Developer action elements:

ATE_COV.2.1D The developer shall provide an analysis of the test coverage.

Content and presentation of evidence elements:

ATE_COV.2.1C The analysis of the test coverage shall demonstrate the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

ATE_COV.2.2C The analysis of the test coverage shall demonstrate that the correspondence between the TSF as described in the functional specification and the tests identified in the test documentation is complete.

Evaluator action elements:

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

ATE_DPT.1 Testing: high-level design

Developer action elements:

ATE_DPT.1.1D The developer shall provide the analysis of the depth of testing.

Content and presentation of evidence elements:

ATE_DPT.1.1C The depth analysis shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the TSF operates in accordance with its high-level design.

Evaluator action elements:

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

ATE_FUN.1 Functional testing

Developer action elements:

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

ATE_FUN.1.2D The developer shall provide test documentation.

Content and presentation of evidence elements:

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.

Evaluator action elements:

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

ATE_IND.2 Independent testing – sample

Developer action elements:

ATE_IND.2.1D The developer shall provide the TOE for testing.

Content and presentation of evidence elements:

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.

Evaluator action elements:

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.

AVA_MSU.2 Validation of analysis

Developer action elements:

AVA_MSU.2.1D The developer shall provide guidance documentation.

AVA_MSU.2.2D The developer shall document an analysis of the guidance documentation.

Content and presentation of evidence elements:

AVA_MSU.2.1C The guidance documentation shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AVA_MSU.2.2C The guidance documentation shall be complete, clear, consistent and reasonable.

AVA_MSU.2.3C The guidance documentation shall list all assumptions about the intended environment.

AVA_MSU.2.4C The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls).

AVA_MSU.2.5C The analysis documentation shall demonstrate that the guidance documentation is complete.

Evaluator action elements:

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

AVA_MSU.2.2E The evaluator shall repeat all configuration and installation procedures, and other procedures selectively, to confirm that the TOE can be configured and used securely using only the supplied guidance documentation.

AVA_MSU.2.3E The evaluator shall determine that the use of the guidance documentation allows all insecure states to be detected.

AVA_MSU.2.4E The evaluator shall confirm that the analysis documentation shows that guidance is provided for secure operation in all modes of operation of the TOE.

AVA_SOF.1 Strength of TOE security function evaluation

Developer action elements:

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.

Strength of Function Declaration:

Two TOE security functions (described in Section 7) SOF are probabilistic in nature. The two functions are:

- DSS keys are restricted and match one DSS .
- Keys to cabinet locks are restricted to installers and administrators.

Both of these security requirements depend upon a limited ability to reproduce or forge a physical key. Two different types of physical keys are used. One type of key fits the DSS Lock and is called the DSS Key. The DSS Key is a traditional shank and tooth design where specific teeth depress lock tumblers. The other type of key fits the Cabinet Lock and is called the Cabinet Key. The Cabinet Key is a “barrel” key type where the key shank is round and hollow. The shank has specific teeth that must line up with slots in the inside the lock barrel. The key is inserted and turned. If all keys are not positioned precisely where lock slots are located, the key will not open the lock. The TOE employs two different types of lock for ease of identification and to minimize the possibility of providing a Cabinet Key to a person who is not authorized access to TSF components.

Since the forgery of both physical keys is of a probabilistic nature, AVA_SOF applies.

The DSS lock employs 14 tumblers allowing 13,950 unique key combinations. The lock uses keys that cannot be duplicated on standard machines for controlled replacements. Key blanks are controlled and are sold only to OEMs and their authorized agents. Each pair of keys has six alphanumeric characters as a serial number, therefore 2,176,782,336 unique key identifiers exist.

The Cabinet Lock has 100,000 possible key positions (barrel key). The serial number of the lock is not externally visible. Cabinet Key pairs have six alphanumeric characters as a serial number, therefore 2,176,782,336 unique key identifiers exist.

The number of distinct keys for either lock in the TOE provides reasonable access control assurance, since the number of unique physical keys used for authentication is incomparable to the number of authentication mechanisms like passwords or encryption tokens. Authentication mechanisms employed at a higher-level of abstraction (like passwords) can be attacked by higher-level abstractions. Therefore, passwords

recognized by operating systems can be attacked by password cracking software. Programs exist that attempt to "guess" a password through intelligent selection that significantly reduces the password space.

With a physical key, an individual has to have access to all keys and try all keys. Such attempts can only occur if the perpetrator has physical access to the TOE. If enough attempts are perpetrated, on the average, an individual will select the correct key on the average of every 6,975 attempts for the DSS Lock and once every 50,000 times for the Cabinet Lock. Since the serial number of either lock is not visible from the outside of the cabinet, each attempt to violate the access control mechanism must be done by attempting to insert the key.

SOF-medium is defined as a level of the TOE strength of function where analysis shows that the function provides adequate protection against straightforward or intentional breach of TOE security by attackers possessing a moderate attack potential.

The overall Strength of Function claim for the TOE is SOF-medium.

Content and presentation of evidence elements:

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.

Evaluator action elements:

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.

AVA_VLA.2 Independent vulnerability analysis

Developer action elements:

AVA_VLA.2.1D The developer shall perform and document an analysis of the TOE deliverables searching for ways in which a user can violate the TSP.

AVA_VLA.2.2D The developer shall document the disposition of identified vulnerabilities.

Content and presentation of evidence elements:

AVA_VLA.2.1C The documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

AVA_VLA.2.2C The documentation shall justify that the TOE, with the identified vulnerabilities, is resistant to obvious penetration attacks.

Evaluator action elements:

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

AVA_VLA.2.2E The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure the identified vulnerabilities have been addressed.

AVA_VLA.2.3E The evaluator shall perform an independent vulnerability analysis.

AVA_VLA.2.4E The evaluator shall perform independent penetration testing, based on the independent vulnerability analysis, to determine the exploitability of additional identified vulnerabilities in the intended environment.

AVA_VLA.2.5E The evaluator shall determine that the TOE is resistant to penetration attacks performed by an attacker possessing a low attack potential.

7 TOE SUMMARY SPECIFICATION (ASE_TSS)

This section presents the security functions implemented by the TOE and the assurance measures applied to ensure their correct implementation, and assurance evidence.

7.1 TOE Security Functions

This section presents the security functions performed by the TOE. To aid evaluation of the TOE, security functions are mapped to SFRs.

Within the SuperNet 2000 EAL4/r1, the TOE Security Functions provide all features necessary to enforce the TSF Security Policy (TSP).
In order for the TSF to enforce the SFP, the TSF must perform the following:

1. Only hardware devices within the workstation that are assigned to a specific UDD receive electrical power when that UDD is selected,
2. Hardware devices not assigned to the selected UDD receive no electrical power
3. UDD selection only can be accomplished through the DSS
4. The DSS can only select one UDD at a time
5. One UDD provides public access, where no authentication device is necessary,
6. One UDD selection requires a physical key authentication device to insert into the DSS
7. DSS Lock matches only the DSS keys delivered with the TOE[5],
8. DSS connections to hardware devices within the workstation cannot be modified, since they are protected by a specially constructed, locked cabinet,
9. Cabinet Lock matches only the cabinet key(s) delivered with the TOE,
10. The TOE has a bright discernable red led that is illuminated when the restricted UDD is selected and another led that is colored green when the public UDD is selected.

Table 9 - Mapping TSF to SFR summarizes the security functional requirements met by the TOE. They are derived verbatim from the Common Criteria Version 2.1 Part 2. Each security functional requirement is mapped to one or more of the ten TSF listed above to demonstrate that if the TSF are provided all of the security functions are met.

Table 9 - Mapping TSF to SFR

CC COMPONENT	NAME	HIERARCHICAL TO	DEPENDENCY	TSF
FDP_ACC.1(a) FDP_ACC.1(b) FDP_ACC.1(c)	Subset access control	None	FDP_ACF.1	3,4,6
FDP_ACF.1(a) FDP_ACF.1(b) FDP_ACF.1(c)	Security attribute based access control	None	FDP_ACC.1 FDP_MSA.3	1,2,3,6
FIA_UAU.1	Timing of authentication	Non	FIA_UID.1	1,2,3,5
FIA_UID.1	Timing of identification	None	None	1,2,3,5
FMT_MOF.1	Management of security functions behavior	None	FMT_SMR.1	9
FMT_MSA.1	Management of Security Attributes	None	FDP_ACC.1 FMT_SMR.1	8
FMT_MSA.3	Static attribute initialization	None	FMT_MSA.1 FMT_SMR.1	7,9
FMT_SMR.1	Security management roles		FIA_UID.1	7,9,10
FPT_PHP.1	Passive detection of physical attack	None	FMT_MOF.1	8
FPT_RVM.1	Non-Bypassability of the TSF	None	None	1,2,3,8
FPT_SEP.1	TSF domain separation	None	None	4, 6

[5] A pair of DSS Keys fit one DSS Lock. Both keys in the pair have the same serial number as the lock. There are 26**6 possible numbers. There are 14,000 possible key configurations.

7.2 TOE States

The following diagram identifies the two possible states in which each individual hardware device can be when the DSS is in one of the three selection positions, Public (P), Interim (I), or Restricted (R). The two states are:

- No Power - No electrical power to the device, for the entire time the DSS position is either in the transition state I or is selecting another hardware domain,
- Operational - As soon as the DSS is placed in a position to select a hardware domain (position P or R) the device specifically connected to the selected DSS position receives electrical power.

It is physically impossible to transition directly from DSS position P to DSS position R, or from position R to position P. All transitions between position P and R must go through the interim DSS position I. All hardware that is dedicated to the P or R UDD experience a power-off condition when transitioning through position I. All hardware that is only operational in DSS position P has no electrical power while the DSS is in position R. All hardware that is only operational in DSS position R has no electrical power to its interface while the DSS is in position P.

Table 10 - DSS States

ALL HARDWARE	DSS POSITION P	DSS POSITION I	DSS POSITION R
Removable hard drive R	No Power	No Power	Operational
NIC card R	No Power	No Power	Operational
Hard drive P	Operational	No Power	No Power
Floppy drive	Operational	No Power	No Power
NIC card P	Operational	No Power	No Power

7.3 Security Functional Requirements

7.3.1 User Data Protection (Class FDP)

This class contains families specifying requirements for TOE security functions and TOE security function policies related to protecting user data.

The TOE satisfies the following families of requirements in this class: FDP_ACC.1 and FDP_ACF.1. The FDP class is discussed below.

7.3.1.1 Subset access control (FDP_ACC.1)

The TOE is physically protected in an environment where users are expected to follow the instructions in the user guide. Within that set of users, information that is available to every user is considered public information. Public information resides in the public UDD only. A subset of users requires access to restricted information and restricted network access. These users are assigned a DSS key that fits one workstation by a customer-authorized administrator. With the DSS key a user can switch the DSS to select the restricted UDD that communicate and permanently store sensitive information.

Access to the inside of the TOE cabinet provides physical access to electric connections that if manipulated incorrectly could cause a violation of the SFP. For this reason entry into the TOE cabinet is protected by a Cabinet Key and access to the Cabinet Key is restricted to an authorized administrator and the installer.

7.3.1.2 Security attribute based access control (FDP_ACF.1)

The DSS is constructed with a lock in it (DSS Lock) such that the DSS can not be turned without first inserting a key into the DSS Lock. The key cannot be removed from the DSS Lock while the DSS is

selecting the Restricted UDD. Once the DSS is switched to the Public switch position, the key can be removed. Customer authorized administrators decide which user is assigned a DSS key for each workstation. The user guide provided by EESI describes the functions of the DSS and site administrators are cautioned concerning its use.

When a user is assigned a DSS Key, the user can switch the DSS to select the Restricted UDD so that all non-shared devices connected to this Restricted UDD DSS switch position become active and all of the non-shared devices connected to the Public UDD DSS position become inactive.

7.3.2 Identification and Authentication (FIA)

Families in this class address the requirements for functions to establish and verify a claimed user identity. Identification and Authentication is required to ensure that users are associated with the proper security attributes.

The TOE satisfies the following families of requirements in this class: FIA_UID.1. This family of functional requirements within the FIA class that are provided by the TOE are discussed below.

7.3.2.1 Timing of Authentication (FIA_UAU.1)

Access to the Public UDD only requires physical access to the TOE, since the DSS, when not in use, only selects the Public DSS and a user first approaches the TOE. If a general user has no DSS Key (cannot be authenticated), then the Public UDD is the only domain available for use. Access to any other object controlled by the TOE requires authentication.

The DSS lock is manufactured by the Illinois Lock Company. The lock is designed for “high security” environments and employs 14 tumblers allowing 13,950 unique key combinations. The DSS lock is turned to operate the DSS and the DSS lock is operated with a DSS Key. The DSS Lock is that part of the DSS that provides an external interface. The DSS Lock is a high-security design in that the DSS provides for a large number of non-repeated key configurations. The serial number of the lock is not externally visible.

7.3.2.2 Timing of identification (FIA_UID.1)

Any user with physical access to the TOE may access the public UDD without first providing identification or authentication.

A user must be in possession of a physical key to assume a trusted role (trusted user, administrator, or installer). If a user is in possession of a DSS Key, the user is either a trusted user who has access to the restricted UDD for a specific workstation or the administrator who has access to more than one workstation. If any higher-level abstractions (e.g. network interfaces, files, operating system) have been accessed on the restricted UDD, the administrator can uniquely identify the user who had access to the restricted UDD.

The DSS lock uses keys that cannot be duplicated on standard machines for controlled replacements. Key blanks are controlled and are sold only to OEMs and their authorized agents. DSS Key pairs have six alphanumeric characters as a serial number, therefore 217,6782,336 unique key identifiers exist.

7.3.3 Security Management (Class FMT)

This class is intended to specify the management of several aspects of the TSF: security attributes, TSF data and functions. The different management roles and their interaction, such as separation of capability, are specified.

The TOE satisfies the following families of requirements in this class: FMT_MOF.1, FMT_MSA.3, and FMT_SMR.1. Each family of functional requirements within the FMT class that are provided by the TOE is discussed below.

7.3.3.1 Management of security functions behavior (FMT_MOF.1)

The TSF restricts the ability to disable, enable, or modify the behavior of the power requirements, domain attachment, or configuration settings of any hardware device to an authorized installer.

The roles that exist at the hardware level interact with the TOE are the “general user,” “trusted user,” “administrator,” and the “installer.” A general user is any individual that has physical access to the operating TOE, since physical access is all that is needed to use the TOE in the unrestricted UDD. A “trusted user” is any user who has in their possession a physical key to be inserted into the DSS to switch the DSS to the restricted UDD. No general user or trusted user is allowed to swap external peripherals or external connections, only administrators and installers are allowed to perform these functions. General and trusted users have no access to hardware devices inside the SuperNet 2000 EAL4/r1 cabinet, because the cabinet is locked, and without the key access must be forced and is noticeable.

An installer is a person who builds a SuperNet 2000 EAL4/r1 at EESI facilities from components as well as a person who may install the SuperNet 2000 EAL4/r1 at a customer site. An installer or an authorized administrator can modify the SuperNet 2000 EAL4/r1 by first taking it out of operation, either at a customer site or at the EESI facilities. Once the TOE is not operable, and installer or an administrator can modify the hardware devices connected to a specific UDD. Only the installer or the administrator can change external connections to the TOE. The installer and the administrator are allowed to change hardware devices and connections inside the TOE.

7.3.3.2 Management of security attributes (FMT_MSA.1)

The TSF enforces the Restricted UDD SFP and restrict the ability to control electrical access to devices connected to the Restricted UDD to trusted users who have in their possession a DSS Key.

The TSF enforces the Authorized Access SFP to restrict the ability to modify electrical connections from the DSS to devices to authorized administrators and installers who have in their possession a Cabinet Key.

7.3.3.3 Static attribute initialization (FMT_MSA.3)

TSF enforces the TOE access control Authorized Access SFP to provide default connection settings for TOE hardware that is used to enforce the Restricted UDD *SFP*.

The TOE physical connections between the DSS and TOE hardware devices that control the Restricted UDD access control SFP are protected inside a specially constructed cabinet. The cabinet is an interlocking design whereby the back must be removed first. The back of the cabinet is secured by a Cabinet Lock that uses a non-reproducible key that is one key in a pair of keys. Both installers and administrators have access to a Cabinet Key. Each Cabinet Lock has two keys, each serial numbered to the lock. An installer has access to one of the two keys and an administrator has access to the other key in the pair.

7.3.3.4 Security Roles (FMT_SMR.1)

The TSF maintains the roles of general user, trusted user, authorized administrator and installer. The TSF is able to associate users with roles. Any person with physical access to the TOE may be a general user, a trusted user, administrator, or an installer. Any person with a key to the DSS is a trusted user. Any person with a Cabinet Key that is reserved, through physical controls, to be assigned to a person in the administrator role is an administrator. Any person with a Cabinet Key that is reserved for installers through physical control, is an installer.

The TSF, in the enforcement of the roles displays a red light to remind the "Trusted User" that they are accessing restricted objects and are operating in an authorized role. Therefore, they must follow the documented guidance provided and protect the restricted UDD accordingly (e.g.. do not leave the key inserted while unattended, always be sure the unrestricted UDD is selected and the key removed before

leaving the workstation unattended). Trusted Users are instructed in the User Guidance to be sure that the red light is not illuminated before leaving the workstation unattended.

7.3.4 Protection of the TSF (Class FPT)

This class contains families of functional requirements that relate to the integrity and management of the mechanisms that provide the TSF (independent of TSP-specifics), and to the integrity of TSF data (independent of the specific contents of the TSP data).

The TOE satisfies the following families of requirements in this class: FPT_PHP.1, FPT_RVM.1, and FPT_SEP.1. The FPT class is discussed below.

7.3.4.1 Passive detection of physical attack (FPT_PHP.1)

For the TOE to protect itself from tampering, the electrical connections between the DSS and UDD hardware devices must be protected from tampering. To do this the TOE employs a specially constructed case. The shell of the case interlocks such that unless forced entry is employed, with visible evidence, access to the connections between the DSS and devices is restricted to authorized administrators and installers. The back of the case is secured with a lock similar to the DSS Lock, and the back of the case must be removed before the sides and the front of the case can be removed exposing the DSS connections. Only EESI installers and customer authorized administrators have access to the Cabinet Key, so only these individuals, in their role, can maintain the electrical configuration of the DSS connections to hardware devices.

Users are instructed to perform a visual inspection of the cabinet for signs of forced entry before using the workstation. If signs of forced entry are evident, users are instructed to immediately contact their security officer and not to attempt to use the workstation.

7.3.4.2 Non-Bypassability of the TSP (FPT_RVM.1)

The TSF ensures that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed. The TSF separates “users” who use the TOE to perform work from individuals who modify and maintain the TOE, installers and administrators. “General” and “trusted users” cannot modify the TSF. This activity is reserved for installers and administrators who are intended to modify the TSF. For “users,” there is only one visible function and that function is controlled by the TSF. This single external interface is switching from one UDD to another UDD by turning the DSS.

A key feature for ensuring the TSP enforcement functions are invoked is the “interim” state that all operating domain transitions must go through. The TSF controls this function and allows it to proceed only if it complies with the TOE access security policy.

All devices with the non-sharable security attribute only receive electrical power (are active) when the DSS selects their associated UDD. All non-sharable devices are inactive in the interim DSS position when transitioning from one UDD to another UDD.

The TSP enforcement functions are hardwired to a physical switch. Upon selecting the other UDD, through the use of the DSS, the TSP enforcement functions are always invoked before any activity can occur in that domain. The DSS is installed such that any tampering with it is easily recognized.

7.3.4.3 Domain separation (FPT_SEP.1)

The TSF maintains a security domain for its own execution that protects it from interference and tampering by untrusted subjects. The DSS is the TOE interface that implements the SFP. The DSS is protected from

modification. Connections between the DSS and the objects it controls also are protected from modification.

The TSF enforces separation between the security domains of subjects in the TSC. The security domain for a user is a specific UDD. The TOE separates these domains for all objects controlled by the TOE. The context switching controlled by the DSS restricts a user to a specific UDD that includes the following: a network connection, disk drives, and a floppy disk drive.

7.4 Assurance Measures

This section identifies the Configuration Management, System Delivery Procedures, System Development Procedures, Guidance Documents, Testing, and Vulnerability Analysis measures associated with the TOE.

7.4.1 Security Assurance Requirements (SARs)

This section outlines the assurance requirement components in this Security Target that were drawn from Part 3 of the Common Criteria necessary to meet the EAL 4 level of assurance. Following the outline, a description of each assurance identified in the outline is included from the Common Criteria for the EAL 4 level of assurance.

7.4.1.1 Configuration Management

The Configuration Management measures applied by EESI specifically identify the TOE and the measures that control all configuration management activities necessary to fully control the design, planning, implementation, testing, fielding and documentation of the TOE

The configuration management system is described in the document, *SuperNet 2000 EAL4/r1 Configuration Management Plan*.

Acceptance procedures that are to be executed at the customer site to ensure the TOE is installed correctly are described in the *SuperNet 2000 Functional Testing and Assembly*.

Assurance Requirements Satisfied: ACM_AUT.1 (Partial CM automation), ACM_CAP.4 (Generation support and acceptance procedures), and ACM_SCP.2 (Problem tracking CM coverage).

7.4.1.2 Delivery and Operation

The delivery and operation of the TOE is controlled sufficiently to ensure that the TOE is installed, generated, and started in the same way the designer and installer intended it to be and that it is delivered without modification. This includes both the procedures taken while the TOE is in transit, as well as the initialization, generation, and start-up procedures.

EESI provides Delivery and Operation documentation in the *SuperNet 2000 EAL4/r1 Delivery and Operation* document and the documents referenced by this document that describes what components are installed in the SuperNet 2000 EAL4/r1 workstation, shipping, packaging, shipping method, delivery records, and installation.

All records are traced by product serial number and there is individual accountability at every step of installation, delivery and installation of the TOE. Every component that when assembled comprises the TOE is identified by the configuration management system described in the *SuperNet 2000 Configuration Management Plan.*

Documents created by the installer that identify every component and the workstation serial number, and the final checkout document travel with the workstation. Once a workstation is shipped, it cannot be internally modified by anyone other than an EESI authorized installer or an administrator unless the

external cabinet suffers forcible entry. Peripheral connections into the back of the workstation that are made at the customer site are performed by an EESI authorized installer. Instructions to place the TOE into operation are provided in the *SuperNet 2000 EAL4/r1 Administrator Guide.*

Installer instructions exist that identify the production flow necessary to build a SuperNet 2000 EAL4/r1 TOE. These instructions are accompanied by drawings and pictures of intermediate installation steps in the installation process.

Instructions for users (both general users and trusted users) provided in the *User Reference Guide* inform users to check the computer case and all external components for visible signs of tampering. Each cable and back-panel connector and product hardware device that is removable has a tag on it. Users are instructed to visually inspect the tag on a cable with the tags on the terminating points of the cable to ensure they match. If a mismatch is found, users are instructed not to use the TOE, and to immediately contact a Administrator.

Assurance Requirements Satisfied: ADO_DEL.2 (Detection of modification), and ADO_IGS.1 (Installation, generation, and start-up procedures).

7.4.1.3 Development

The development assurance components for EAL4 have been completed by EESI. These components include: fully defined external interfaces, Functional Specification, High-Level Design, Low-Level Design, an informal correspondence demonstration, and an informal TOE security policy model.

7.4.1.3.1 Fully-defined external interfaces

External interfaces to the TOE are identified in the *SuperNet 2000 EAL4/r1Functional Specification* provided by EESI. The *SuperNet 2000 EAL4/r1Functional Specification* provided by EESI provides the following information:

- Describes the TSF and its external interfaces using an informal style.
- It is internally consistent.
- Describes the purpose and method of use of all external TSF interfaces, providing complete details of all effects, exceptions and error messages.
- Completely represents the TSF.
- Includes rationale that the TSF is completely represented.

7.4.1.3.2 High-level design

The *SuperNet 2000 EAL4/r1 High-Level Design* document describes the structure of the TSF informally. Since the availability of electrical power to devices is how the SFP is enforced, TSF subsystems are associated with device objects being available through the manipulation of electrical power. All interfaces are categorized relative to their ability to operate at all because of the availability of electrical power.

7.4.1.3.3 Implementation Representation

The TOE is entirely comprised of hardware. The entire TOE implementation is available for review and analysis. All hardware is described in the *SuperNet 2000 EAL4/r1 High-Level Design,* and the *SuperNet 2000 EAL4/r1 Low-Level Design.*.

7.4.1.3.4 Descriptive low-level design

The TOE is a hardware switch that provides or denies electrical power to devices, therefore the modules are the hardware objects that are controlled by the DSS. A Low-level design document, the *SuperNet 2000 EAL4/r1 Low-Level Design*, is provided that informally describes the following:

- the TSF in terms of modules,

- the purpose of each module,
- the interrelationships between the modules in terms of provided security functionality and dependencies on other modules,
- how each TSP-enforcing function is provided,
- all interfaces to the modules of the TSF,
- which of the interfaces to the modules of the TSF are externally visible,
- purpose and method of use of all interfaces to the modules of the TSF,
- separation of the TOE into TSP-enforcing and other modules.

7.4.1.3.5 Informal Correspondence Demonstration

The correspondence between all adjacent pairs of TSF representations is described in the documents that describe a TSF representation. Therefore the demonstration of correspondence is provided by the *SuperNet 2000 EAL4/r1 Security Target, SuperNet 2000 EAL4/r1 Functional Specification, SuperNet 2000 EAL4/r1 High-Level Design,* and the *SuperNet 2000 EAL4/r1 Low-Level Design.* For each adjacent pair of provided TSF representations, the analysis demonstrates that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

This Security Target provides correspondence between threats and objectives, objectives and functional requirements, assurance categories and assurance requirements in the Rationale Section.

7.4.1.3.6 Informal TOE Security Policy Model

EESI has completed an informal TSP model that demonstrates correspondence between the functional specification and the TSP model. The TSP model describes the rules and characteristics of all policies of the TSP that can be modeled. The TSP model includes a rationale that demonstrates that it is consistent and complete with respect to all policies of the TSP that can be modeled. The demonstration of correspondence between the TSP model and the functional specification shows that all of the security functions in the functional specification are consistent and complete with respect to the TSP model.

The *SuperNet 2000 EAL4/r1* informally describe the TOE security policy model.

Assurance Requirements Satisfied: ADV_FSP.2 (Fully defined external interfaces), ADV_HLD.2 (Security enforcing high-level design), ADV_IMP.1 (Subset of Implementation of the TSF), ADV_LLD.1 (Descriptive low-level design), ADV_RCR.1 (Informal Correspondence demonstration), and ADV_SPM.1 (Informal TOE security policy model).

7.4.1.4 Guidance Documents

The Guidance Documents provided by EESI include both Installation and Configuration manuals that guide Installers through the process of building the TOE and installing the product correctly.

Three guidance documents are provided with the TOE. A *User Quick Reference Guide* is a one-page card that provides a user with a quick reference to use. The *User Reference Guide* is a more complete document that provides a user with the necessary information to use the TOE . The *Administrative Guide* provides the administrator the information needed to install and maintain the TOE

Assurance Requirements Satisfied: AGD_ADM.1 (Administrator Guidance), AGD_USR.1 (User Guidance).

7.4.1.5 Life-Cycle Support

7.4.1.5.1 Security Documentation

EESI has developed security documentation that describes all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment. This documentation provides evidence that these security measures are followed during the development and maintenance of the TOE.

The documents are: the *SuperNet 2000 EAL4/r1 Configuration Management Plan,* the *SuperNet 2000 EAL4/r1 Functional Testing and Assembly, and the SuperNet 2000 EAL4/r1 Delivery and Operation.*

7.4.1.5.2 Life-cycle model

EESI has established a life-cycle model that is used in the development and maintenance of the TOE. This model describes a life-cycle model to develop and maintain the TOE, and one that provides necessary control over the development and maintenance of the TOE.

The EESI life-cycle definition documentation describes the model used to develop and maintain the TOE, explains why the model was chosen, explains how the model is used to develop and maintain the TOE, and demonstrates compliance with the life-cycle model.

The document that describes the life-cycle model is the *SuperNet 2000 EAL4/r1 Functional Testing and Assembly.*

7.4.1.5.3 Development tools

The development tools used by EESI to develop the TOE are well defined and the method used to select implementation option is well defined and understood by all developers

The document that describes the development tools is the *SuperNet 2000 EAL4/r1 Functional Testing and Assembly.*.

Assurance Requirements Satisfied: ALC_DVS.1 (Identification of security measures), ALC_LCD.1 (Developer defined life-cycle model), ALC_TAT.1(Well-defined development tools).

7.4.1.6 Testing

7.4.1.6.1 Test Coverage

EESI has completed an analysis of test coverage to determine that all tests identified and the TSF described in the functional specification are tested.

The document that describes test coverage is the *SuperNet 2000 EAL4/r1 Test Plan.*

7.4.1.6.2 Testing: high-level design

EESI has provided an analysis of tests that demonstrates that the tests identified in the test documentation are sufficient to demonstrate that the TSF operates in accordance with its high-level design.

The document that describes test coverage is the *SuperNet 2000 EAL4/r1 Test Plan Procedures* and the *SuperNet 2000 EAL4/r1 Functional Testing and Assembly.*

7.4.1.6.3 Functional Testing

EESI has completed test documentation that describes test plans, test procedure descriptions, expected test results and actual test results, the security functions to be tested and describe the goal of the tests to be performed.

The test procedure descriptions identify the tests to be performed and describe the scenarios for testing each security function. The expected test results show the anticipated outputs from a successful execution of the tests and the actual test results from the developer execution of the tests demonstrate that each tested security function behaved as specified.

The documents that describe functional testing are: the *SuperNet 2000 EAL4/r1 Test Plan* the *SuperNet 2000 EAL4/r1 Test Procedures* and the *SuperNet 2000 EAL4/r1 Functional Testing and Assembly*.

7.4.1.6.4 Independent Testing

EESI will provide the TOE for testing and the TOE will provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

Assurance Requirements Satisfied: ATE_COV.2 (Analysis of coverage), ATE_DPT.1 (Testing: high-level design), ATE_FUN.1 (Functional Testing), ATE_IND.2 (Independent testing – sample.

7.4.1.7 Vulnerability Analysis

7.4.1.7.1 Vulnerability Analysis

The DSS lock is manufactured by the Illinois Lock Company. The lock is designed for "high security" environments like cash boxes and safety-deposit boxes. The lock employs 14 tumblers allowing 13,950 unique key combinations. The lock uses keys that cannot be duplicated on standard machines for controlled replacements. Key blanks are controlled and are sold only to OEMs and their authorized agents. Each pair of keys has six alphanumeric characters as a serial number, therefore 217,6782,336 unique key identifiers exist.

13,950 distinct key positions provides reasonable access control assurance since the number of unique physical keys used for authentication is incomparable to the number of authentication mechanisms like passwords. Authentication mechanisms employed at a higher-level of abstraction (like passwords) can be attacked by higher-level abstractions. Therefore, passwords recognized by operating systems can be attacked by password cracker software. Programs exist that attempt to "guess" a password through intelligent selection that significantly reduces the password space.

With a physical key, an individual has to have access to all keys and try all keys. If enough attempts are perpetrated, on the average, an individual will select the correct key on the average of every 6,975 attempts. Since the serial number of the lock is not visible from the outside of the cabinet, each key entry attempt must be done by attempting to insert the key.

The Cabinet Lock is manufactured by the Forte Lock Company. It has 100,000 possible key positions (barrel key). Each Cabinet Lock has two serial-numbered keys. The serial number of the lock is not externally visible. Cabinet Key pairs have six alphanumeric characters as a serial number, therefore 217,6782,336 unique key identifiers exist.

EESI has documented its vulnerability assessment in the *SuperNet 2000 EAL4/r1 Vulnerability Assessment* document.

7.4.1.7.2 Validation of Analysis

EESI has developed the *SuperNet 2000 EAL4/r1 Vulnerability Assessment* document that describes the assement for potential vulnerabilities, misuse analysis, strength of function analysis, and the vulnerability analysis. The Vulnerability Assessment looks at the guidance information and presents an analysis that demonstrates that the guidance documentation is complete.

Documents include: *SuperNet 2000 EAL4/r1 Vulnerability Assessment.*

7.4.1.7.3 Independent Vulnerability Analysis

EESI has performed and documented an analysis of the TOE deliverables searching for ways in which a user can violate the TSP. EESI has documented each hypothesized vulnerability and that the vulnerability cannot be exploited in the intended environment for the TOE.

The document that describes the Vulnerability Analysis is the *SuperNet 2000 EAL4/r1 Vulnerability Assessment.*

Assurance Requirements Satisfied: AVA_MSU.2 (Validation of analysis), AVA_VLA.2 ((Independent vulnerability analysis)

7.5 Assurance Evidence

This section outlines the documents from EESI that support the assurance claims made for the TOE. Table 11 - EAL4 Assurance Evidence identifies all documents that satisfy or participate in the satisfaction of a specific assurance requirement.

Table 11 - EAL4 Assurance Evidence

ASSURANCE CLASS	ASSURANCE COMPONENTS	EVIDENCE
Configuration Management	ACM_AUT.1 Partial CM automation	SuperNet 2000 EAL4/r1 Configuration Management Plan
	ACM_CAP.4 Generation support and acceptance procedures	SuperNet 2000 EAL4/r1 Functional Testing and Assembly SuperNet 2000 EAL4/r1 Configuration Management Plan
	ACM_SCP.2 Problem tracking CM coverage	SuperNet 2000 EAL4/r1 Configuration Management Plan
Delivery and Operation	ADO_DEL.2 Detection of modification	SuperNet 2000 EAL4/r1 Delivery and Operation SuperNet 2000 EAL4/r1 Administration Guide SuperNet 2000 EAL4/r1Configuration Management Plan SuperNet 2000 EAL4/r1 User Reference Guide
	ADO_IGS.1 Installation, generation, and start-up procedures	SuperNet 2000 EAL4/r1 Administration Guide SuperNet 2000 EAL4/r1 Delivery and Operation
Development	ADV_FSP.2 Fully defined external interfaces	SuperNet 2000 EAL4/r1 Functional Specification
	ADV_HLD.2	SuperNet 2000 EAL4/r1 High-Level Design
	ADV_IMP.1 Subset of Implementation of the TSF	SuperNet 2000 EAL4/r1 High-Level Design SuperNet 2000 EAL4/r1 Low-Level Design
	ADV_LLD.1 Descriptive low-level design	SuperNet 2000 EAL4/r1 Low-Level Design
	ADV_RCR.1 Informal Correspondence demonstration	SuperNet 2000 EAL4/r1 Security Target SuperNet 2000 EAL4/r1 Functional Specification SuperNet 2000 EAL4/r1 High-Level Design SuperNet 2000 EAL4/r1 Low-Level Design
	ADV_SPM.1 Informal TOE security policy model	SuperNet 2000 EAL4/r1 Security Target
Guidance Documents	AGD_ADM.1 Administrator guidance	SuperNet 2000 EAL4/r1 Administrator Guide
	AGD_USR.1 User guidance	SuperNet 2000 EAL4/r1 Quick Reference Guide SuperNet 2000 EAL4/r1 User Reference Guide
Life Cycle Support	ALC_DVS.1 Identification of security measures	SuperNet 2000 EAL4/r1 Functional Testing and Assembly SuperNet 2000 EAL4/r1 Configuration Management Plan SuperNet 2000 EAL4/r1 Delivery and Operation
	ALC_LCD.1 Developer defined life-cycle model	SuperNet 2000 EAL4/r1 Functional Testing and Assembly
	ALC_TAT.1 Well-defined development tools	SuperNet 2000 EAL4/r1 Functional Testing and Assembly
Tests	ATE_COV.2 Analysis of coverage	SuperNet 2000 EAL4/r1 Test Plan
	ATE_DPT.1 Testing: high-level design	SuperNet 2000 EAL4/r1 Functional Testing and Assembly SuperNet 2000 EAL4/r1 Test Plan
	ATE_FUN.1 Functional testing	SuperNet 2000 EAL4/r1 Functional Testing and Assembly SuperNet 2000 EAL4/r1 Test Plan SuperNet 2000 EAL4/r1 Test Procedures
Vulnerability Assessment	AVA_MSU.2 Validation of analysis	SuperNet 2000 EAL4/r1 Vulnerability Assessment
	AVA_SOF.1 Strength of TOE security function evaluation	SuperNet 2000 EAL4/r1 Vulnerability Assessment
	AVA_VLA.2 Independent vulnerability analysis	SuperNet 2000 EAL4/r1 Vulnerability Assessment

8 RATIONALE

This section presents the evidence used in the ST evaluation. This evidence supports the claims that the ST is a complete and cohesive set of requirements, that a conformant TOE would provide an effective set of IT security countermeasures within the security environment, and that the TOE summary specification addresses the requirements.

8.1 Rationale for IT Security Objectives

Table 12 - Mapping Security Objectives to Assumptions and Threats identifies the TOE security objectives, provides a brief description of each objective, and maps each objective to the threats that is to be addressed by the objective. Also in Table 12 are the assumptions that apply for an objective to fully address the threats to which the objective applies.

Table 12 - Mapping Security Objectives to Assumptions and Threats

OBJECTIVE	DESCRIPTION	ASSUMPTIONS OR THREATS
O.BYPASS	Users can only select the UDD by manually using the DSS.	T. SENSITIVE
O.CONFIGURATION	The TOE will protect configuration settings from being altered by any individual other than an Installer or the Administrator.	A.ADMIN A.NOEVIL, A.PHYSICAL, T.CABINET_COMPROMISE, T.CONFIGURATION T.SPOOF
O.DETECT	Unauthorized physical entry into the TOE cabinet shall be detectable by a user.	A.SECURITY-AWARE, T.CABINET_COMPROMISE
O.FLOPPY	The TOE will prevent the availability of a floppy in the transition state and in one of the two hardware environments.	A.ELECTRICAL T.SWITCH_FAILURE
O.INDICATE	A user receives an unambiguous indication of which domain has been selected.	T.DSS_COMPROMISE T.SPOOF
O.ISOLATE	TOE shall isolate one hardware domain from another domain so that no electrical power is provided to hardware connected to a UDD not selected by the DSS.	A.MODIFY T.NETWORK_ISOLATE T.SWITCH_FAILURE
O.MODIFY	Only an EESI designated installer or customer designated administrator may install, modify and repair connections inside the TOE case. These connections are between the DSS and specific hardware devices.	A.ADMIN A.MODIFY
O.RESTRICTED_ACCESS	Access to the restricted UDD is limited to users in possession of the physical DSS key that is paired to the specific DSS.	A.KEY A.PHYSICAL A.TRUSTED T.SENSITIVE T.SENSITIVE T.SWITCH_FAILURE
O.SELECT	An explicit action by the user is used to select the domain to which the set of devices is connected. Single rotary selection is used..	T.SPOOF

8.2 Rationale for Environmental Security Objectives

Certain objectives with respect to the general operating environment must be met. The following are the TOE's environmental security objectives and the assumptions they meet:

Table 13 - Environmental Security Threats

OBJECTIVE	DESCRIPTION	ASSUMPTIONS
O.E.ENVIRON	The TOE environment must be appropriate to facilitate proper operation and maintenance and it must be maintained in accordance with this objective.	A.ADMIN A.MODIFY, A.PHYSICAL, A.SECURITY-AWARE T.E.PHYSICAL
O.INSTALL	Those responsible for the TOE must ensure that the TOE is installed, managed, and operated in a manner which maintains IT security.	A.ADMIN A.NOEVIL T.E.ADMIN
O.E.MANUAL.LOG	A manual record is maintained by a customer security officer that identifies which users have been assigned a DSS Key and/or a Cabinet Key	A.KEYS T.CONFIGURATION T.SENSITIVE
O.E.PHYSICAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from physical attack that might compromise IT security..	T.E.PHYSICAL, A.ADMIN A.PHYSICAL A.TRUSTED

8.3 Rationale for Security Functional Requirements

Discussions of the rationale for specific security requirements was included in the section discussing TOE Security Requirements, rather than introduce security requirements in one section and discuss their rationale later in the Security Target. Below is a matrix that maps TOE Security Functional Requirements and IT Security Objectives.

Table 14 - Security Functional Requirements

CC COMPONENT	NAME	HIERARCHICAL TO	DEPENDENCY	OBJECTIVES FUNCTION HELPS ADDRESS
FDP_ACC.1(a) FDP_ACC.1(b) FDP_ACC.1(c)	Subset access control	None	FDP_ACF.1	O.CONFIGURATION
FDP_ACF.1(a) FDP_ACF.1(b) FDP_ACF.1(c)	Security attribute based access control	None	FDP_ACC.1 FDP_MSA.3	O.CONFIGURATION O.MODIFY O.RESTRICTED_ACCESS
FIA_UAU.1	Timing of authentication	Non	FIA_UID.1	O.MODIFY O.RESTRICTED_ACCESS
FIA_UID.1	Timing of identification	None	None	O.CONFIGURATION O.SELECT
FMT_MOF.1	Management of security functions behavior	None	FMT_SMR.1	O.CONFIGURATION
FMT_MSA.1	Management of Security Attributes	None	FDP_ACC.1 FMT_SMR.1	O.CONFIGURATION
FMT_MSA.3	Static attribute initialization	None	FMT_MSA.1 FMT_SMR.1	O.CONFIGURATION
FMT_SMR.1	Security management roles	None	FIA_UID.1	O.E.PHYSICAL
FPT_PHP.1	Passive detection of physical attack	None	FMT_MOF.1	O.DETECT
FPT_RVM.1	Non-Bypassability of the TSF	None	None	O.BYPASS O.CONFIGURATION O.FLOPPY O.ISOLATE O.SELECT
FPT_SEP.1	TSF domain separation	None	None	O.CONF O.INDICATE O.ISOLATE

8.4 Assurance Requirements

EAL4 was chosen to provide a moderate to high level of independently assured security, since the TSF is not complex, the TSP is a simple one and the TSP is enforced at the hardware level. EAL4 permits a customer to gain TOE assurance from positive engineering based on good commercial development practices, which though rigorous, do not require substantial specialized knowledge, skills, and other

resources. The environment in which the SuperNet 2000 EAL4/r1 is designed and implemented is a sound engineering environment. EESI is a small business, where the president of the company is professional trained Electrical Engineer who designed the TOE and maintains control over all modification. The design staff are all trained engineers or technicians. This environment is a reasonable development and implementation environment considering the TOE is a hardware switch and the hardware devices to which the switch provides electrical power.

Table 15 - Assurance Classes Satisfied identifies the assurance classes for which TOE compliance has been identified in this Security Target.

Table 15 - Assurance Classes Satisfied

ASSURANCE CLASS	ASSURANCE COMPONENTS
Configuration Management	ACM_AUT.1 Partial CM automation
	ACM_CAP.4 Generation support and acceptance procedures
	ACM_SCP.2 Problem tracking CM coverage
Delivery and Operation	ADO_DEL.2 Detection of modification
	ADO_IGS.1 Installation, generation, and start-up procedures
Development	ADV_FSP.2 Fully defined external interfaces
	ADV_HLD.2
	ADV_IMP.1 Subset of Implementation of the TSF
	ADV_LLD.1 Descriptive low-level design
	ADV_RCR.1 Informal Correspondence demonstration
	ADV_SPM.1 Informal TOE security policy model
Guidance Documents	AGD_ADM.1 Administrator guidance
	AGD_USR.1 User guidance
Life Cycle Support	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.1 Well-defined development tools
Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: high-level design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
Vulnerability Assessment	AVA_MSU.2 Validation of analysis
	AVA_SOF.1 Strength of TOE security function evaluation
	AVA_VLA.2 Independent vulnerability analysis

8.5 Internal Consistency and Mutually Supportive Rationale

The set of security requirements provided in this Security Target for the SuperNet 2000 EAL4/r1 TOE form a mutually supportive and internally consistent description, since security threats have been identified that have been countered with objectives for the TOE. These objectives have been refined to security requirements that meet those objectives. All requirement dependencies have been met, and requirements do not contradict each other. Through correspondence discussions, it has been demonstrated that all security functional requirements are met by the TOE security functions. Security functions have been further refined into subsystems. Each level of refinement has been documented and reviewed for consistency. Finally, it has been shown that all EAL4 assurance requirements have been met demonstrating that that the assurance claim that the TOE meets the security requirements is consistent with the claims in the Security Target.