Peripheral Sharing Switch (PSS)

for Human Interface Devices

Protection Profile

Version 1.0
8 August 2000

National Security Agency
9800 Savage Road
Fort George G. Meade, MD 20755-6704

This document is consistent with the
Common Criteria for Information Technology Security Evaluation
Version 2.1
(CCIMB-99-031, August 1999)
at *Evaluation Assurance Level 4*

Table of Contents

Foreword 4

1. Introduction 5
   1.1 Identification. . . . 5
   1.2 Protection Profile Overview 5

2. Target of Evaluation Description 6
   Data Separation Security Function Policy (SFP) 6
   Figure 1: A Typical Configuration of Shared Peripherals 7

3. Target of Evaluation Security Environment 8
   3.1 Secure Usage Assumptions 8
   3.2 Threats to Security 9

4. Security Objectives 10
   4.1 Security Objectives for the Target of Evaluation 10
   4.2 Security Objectives for the Environment 11

5. Information Technology Security Requirements 12
   5.1 Target of Evaluation Security Functional Requirements 12
      5.1.1 User Data Protection (FDP) 12
         Switching Rule 12
      5.1.2 Security Management (FMT) 13
      5.1.3 Protection of the TOE Security Functions (FPT). . . . 14
      5.1.4 Extended Requirements (EXT). . . . 14
         Visual Indication Rule 14
   5.2 Target of Evaluation Security Assurance Requirements 15
      5.2.1 Configuration Management (ACM) 15
      5.2.2 Delivery and Operation (ADO) 17
      5.2.3 Development (ADV) 18
      5.2.4 Guidance Documents (AGD) 22
      5.2.5 Life Cycle Support (ALC) 23
      5.2.6 Tests (ATE) 25
      5.2.7 Vulnerability Assessment (AVA) 27

Table of Contents

(Continued)

6. Rationale 30
6.1 Security Objectives Rationale 30
6.2 Security Requirements Rationale 32
6.3 Dependencies Not Met 34
6.4 Mapping Tables 35
Table 1: Mapping of Threats to Objectives 35
Table 2: Mapping of Security Functional Requirements to Objectives 36
Table 3: Mapping of Security Functional Requirements Dependencies . . .37

Terms of Reference. 38

Acronyms 42

References 44

Foreword

This publication, “Peripheral Sharing Switch (PSS) for Human Interface Devices” Protection Profile, is issued by the Information Systems Security Organization (ISSO) as part of its program to promulgate security standards for the components of information assurance solutions.

The base set of requirements used in this Protection Profile are taken from the *Common Criteria for Information Technology Security Evaluation*, Version 2.1. Further information, including the status and updates, of both this Profile and the Common Criteria, can be found on the Internet at “http://www.radium.ncsc.mil/tpep”.

Words which appear in SMALL CAPITALS are those which are formally defined in the Terms of Reference section.

Comments on this document should be directed to:

PSS PP Team (C43)
National Security Agency
9800 Savage Road, Suite 6704
Fort George G. Meade, MD 20755-6704

or

sjhirsc@thematirx.ncsc.mil

or

(410) 854-6191

1. Introduction

1.1 Identification

Title: Peripheral Sharing Switch (PSS) for Human Interface Devices.

Assurance Level: EAL 4.

PP Version: 1.0, 8 August 2000.

General Status: Evaluated Products List.

Registration: PSSPP;
NSA/Information Systems Security Organization.

Keywords: DEVICE sharing, multi-way SWITCH, PERIPHERAL switching, KEYBOARD-Video-MONITOR/Mouse (KVM) SWITCH.

1.2 Protection Profile Overview

This Protection Profile specifies U.S. Department of Defense minimum security requirements for PERIPHERAL SWITCHES; DEVICES which enable a single set of HUMAN INTERFACE DEVICES to be shared between multiple COMPUTERS.

The Protection Profile is consistent with Common Criteria Version 2.1:
Part 2 extended, and
Part 3 conformant (Evaluation Assurance Level 4).

2. Target of Evaluation Description

This document addresses a DEVICE, hereinafter referred to as a “Peripheral Sharing Switch” (PSS) or simply “SWITCH”--the Target of Evaluation (TOE)--permitting a single set of HUMAN INTERFACE DEVICES to be shared among two or more COMPUTERS (see Figure 1).

The TOE is normally installed in settings where a single USER with limited work surface space needs to access two or more COMPUTERS, collectively termed *SWITCHED COMPUTERS* (which need not be physically distinct entities). The USER may have a KEYBOARD, a visual display (e.g., MONITOR), a POINTING DEVICE (e.g., mouse), and/or alternative INPUT/OUTPUT DEVICES to interact with the COMPUTER(S). These are collectively referred to as the *SHARED PERIPHERALS*.

In operation, the TOE will be CONNECTED to only one COMPUTER at a time. To use a different COMPUTER, the USER must perform some specific action (e.g., push a button, turn a knob, etc.). The TOE will then visually indicate which COMPUTER was selected by the USER. Such indication is persistent and not transitory in nature.

The TOE must not have, and in fact must specifically preclude, any features that permit USER information to be shared or transferred between COMPUTERS via the TOE.

A PERIPHERAL PORT GROUP is a collection of DEVICE PORTS treated as a single entity by the TOE. There is one GROUP for the set of SHARED PERIPHERALS and one GROUP for each CONNECTED SWITCHED COMPUTER. Each SWITCHED COMPUTER GROUP has some unique associated logical ID. The SHARED PERIPHERAL GROUP ID is considered to be the same as that of the SWITCHED COMPUTER GROUP currently selected by the TOE.

Data Separation Security Function Policy (SFP):

> *The TOE shall allow PERIPHERAL DATA and STATE INFORMATION to be transferred only between PERIPHERAL PORT GROUPS with the same ID.*

The TOE itself is not concerned with the USER’S information flowing between the SHARED PERIPHERALS and the SWITCHED COMPUTERS. It is only providing a CONNECTION between the HUMAN INTERFACE DEVICES and a selected COMPUTER at any given instant.

SWITCHES of this type may differ significantly from the familiar “A/B” printer or serial port SWITCHES, where no constraints are placed on connections between devices. Some SWITCHES may provide enhanced features such as scanning (where it continually switches between the COMPUTERS until the USER performs an action to halt the switching), or video protocol conversion (e.g., Macintosh, Sun, PC, etc.) information in mixed COMPUTER environments. These enhancements must be examined to insure that information is not shared or transferred between COMPUTERS.

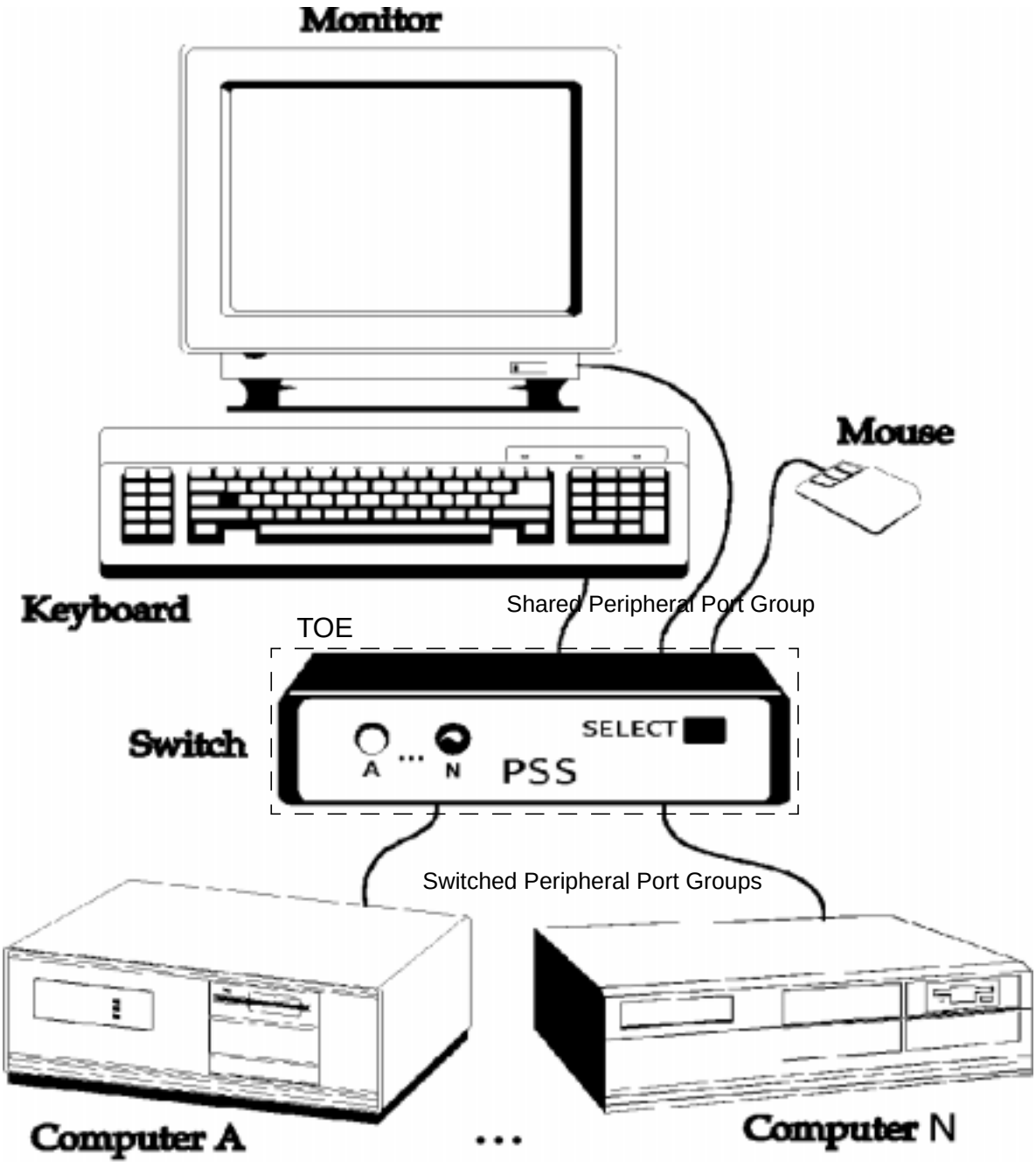

Figure 1: A Typical Configuration of Shared Peripherals

3. Target of Evaluation Security Environment

3.1 Secure Usage Assumptions

A.ACCESS An AUTHORIZED USER possesses the necessary privileges to access the information transferred by the TOE.

USERS are AUTHORIZED USERS.

A.EMISSION The TOE meets the appropriate national requirements (in the country where used) for conducted/radiated electromagnetic emissions. [In the United States, *Part 15 of the FCC Rules for Class B digital devices*.]

A.ISOLATE Only the selected COMPUTER'S video channel will be visible on the shared MONITOR.

A.MANAGE The TOE is installed and managed in accordance with the manufacturer's directions.

A.NOEVIL The AUTHORIZED USER is non-hostile and follows all usage guidance.

A.PHYSICAL The TOE is physically secure.

A.SCENARIO Vulnerabilities associated with attached DEVICES (SHARED PERIPHERALS or SWITCHED COMPUTERS), or their CONNECTION to the TOE, are a concern of the application scenario and not of the TOE.

3.2 Threats to Security

The asset under attack is the information transiting the TOE.
In general, the threat agent is most likely (but not limited to) people with TOE access (who are expected to possess “average” expertise, few resources, and moderate motivation) or failure of the TOE or PERIPHERALS.

T.BYPASS The TOE may be bypassed, circumventing nominal SWITCH functionality.

T.INSTALL The TOE may be delivered and installed in a manner which violates the security policy.

T.LOGICAL The functionality of the TOE may be changed by reprogramming in such a way as to violate the security policy.

T.PHYSICAL A physical attack on the TOE may violate the security policy.

T.RESIDUAL RESIDUAL DATA may be transferred between PERIPHERAL PORT GROUPS with different IDs.

T.SPOOF Via intentional or unintentional actions, a USER may think the set of SHARED PERIPHERALS are CONNECTED to one COMPUTER when in fact they are connected to a different one.

T.STATE STATE INFORMATION may be transferred to a PERIPHERAL PORT GROUP with an ID other than the selected one.

T.TRANSFER A CONNECTION, via the TOE, between COMPUTERS may allow information transfer.

4. Security Objectives

4.1 Security Objectives for the Target of Evaluation

O.CONF The TOE shall not violate the confidentiality of information which it processes.

Information generated within any PERIPHERAL GROUP-COMPUTER CONNECTION shall not be accessible by any other PERIPHERAL GROUP-COMPUTER CONNECTION.

O.CONNECT No information shall be shared between SWITCHED COMPUTERS via the TOE.

This includes STATE INFORMATION, if such is maintained within the TOE.

O.INDICATE The AUTHORIZED USER shall receive an unambiguous indication of which SWITCHED COMPUTER has been selected.

O.INVOKE Upon switch selection, the TOE is invoked.

O.NOPROG Logic contained within the TOE shall be protected against unauthorized modification.

Embedded logic must not be stored in programmable or re-programmable components.

O.ROM TOE software/firmware shall be protected against unauthorized modification.

Embedded software must be contained in mask-programmed or one-time-programmable read-only memory permanently attached (non-socketed) to a circuit assembly.

O.SELECT An explicit action by the AUTHORIZED USER shall be used to select the COMPUTER to which the shared set of PERIPHERAL DEVICES is CONNECTED.

Single push button, multiple push button, or rotary selection methods are used by most (if not all) current market products.

Automatic switching based on scanning shall not be used as a selection mechanism.

O.SWITCH All DEVICES in a SHARED PERIPHERAL GROUP shall be CONNECTED to at most one SWITCHED COMPUTER at a time.

4.2 Security Objectives for the Environment

All of the Secure Usage Assumptions are considered to be Security Objectives for the Environment. These Objectives are to be satisfied without imposing technical requirements on the TOE; they will not require the implementation of functions in the TOE hardware and/or software, but will be satisfied largely through application of procedural or administrative measures.

OE.ACCESS The AUTHORIZED USER shall possess the necessary privileges to access the information transferred by the TOE.

USERS are AUTHORIZED USERS.

OE.EMISSION

The TOE shall meet the appropriate national requirements (in the country where used) for conducted/radiated electromagnetic emissions. [In the United States, *Part 15 of the FCC Rules for Class B digital devices.]*

OE.ISOLATE Only the selected COMPUTER'S video channel shall be visible on the shared MONITOR.

OE.MANAGE The TOE shall be installed and managed in accordance with the manufacturer's directions.

OE.NOEVIL The AUTHORIZED USER shall be non-hostile and follow all usage guidance.

OE.PHYSICAL

The TOE shall be physically secure.

OE.SCENARIO

Vulnerabilities associated with attached DEVICES (SHARED PERIPHERALS or SWITCHED COMPUTERS), or their CONNECTION to the TOE, shall be a concern of the application scenario and not of the TOE.

5. Information Technology Security Requirements

5.1 Target of Evaluation Security Requirements

Words which appear in *italics* are tailorings (via permitted operations) of requirement definitions.

5.1.1 User Data Protection (FDP)

5.1.1.1 **FDP_ETC.1** (Export of User Data Without Security Attributes)
[Dependencies: FDP_ACC.1 or FDP_IFC.1]

1 The TSF shall enforce the *Data Separation SFP* when exporting user data, controlled under the SFP(s), outside of the TSC.

2 The TSF shall export the user data without the user data's associated security attributes.

5.1.1.2 **FDP_IFC.1** (Subset Information Flow Control)
[Dependencies: FDP_IFF.1]

1 The TSF shall enforce the *Data Separation SFP* on
the set of PERIPHERAL PORT GROUPS, *and*
the bi-directional flow of PERIPHERAL DATA *and* STATE INFORMATION *between the* SHARED PERIPHERALS *and the* SWITCHED COMPUTERS.

5.1.1.3 **FDP_IFF.1** (Simple Security Attributes)
[Dependencies: FDP_IFC.1 and FMT_MSA.3]

1 The TSF shall enforce the *Data Separation SFP* based on the following types of subject and information security attributes:
PERIPHERAL PORT GROUPS (SUBJECTS),
PERIPHERAL DATA *and* STATE INFORMATION (OBJECTS), *and*
PERIPHERAL PORT GROUP *IDs (*ATTRIBUTES*).*

2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

Switching Rule:
*P*ERIPHERAL DATA *can flow to a* PERIPHERAL PORT GROUP *with a given ID only if it was received from a* PERIPHERAL PORT GROUP *with the same ID.*

3 The TSF shall enforce the
[No additional information flow control SFP rules.]

4 The TSF shall provide the following:
[No additional SFP capabilities.]

5 The TSF shall explicitly authorise an information flow based on the following rules:
[No additional rules.]

6 The TSF shall explicitly deny an information flow based on the following rules:
[No additional rules.]

5.1.1.4 **FDP_ITC.1** (Import of User Data Without Security Attributes)
[Dependencies: (FDP_ACC.1 or FDP_IFC.1) and FMT_MSA.3]

1 The TSF shall enforce the *Data Separation SFP* when importing user data, controlled under the SFP, from outside the TSC.

2 The TSF shall ignore any security attributes associated with the user data when imported from outside the TSC.

3 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC:
[No additional rules.]

5.1.2 Security Management (FMT)

5.1.2.1 **FMT_MSA.1** (Management of Security Attributes)
[Dependencies: (FDP_ACC.1 or FDP_IFC.1) and FMT_SMR.1]

1 The TSF shall enforce the *Data Separation SFP* to restrict the ability to *modify* the security attributes *PERIPHERAL PORT GROUP IDS* to *the USER.*

Application Note: An AUTHORIZED USER shall perform an explicit action to select the COMPUTER to which the shared set of PERIPHERAL devices is CONNECTED.

5.1.2.2 **FMT_MSA.3** (Static Attribute Initialisation)
[Dependencies: FDP_MSA.1 and FMT_SMR.1]

1 The TSF shall enforce the *Data Separation SFP* to provide *restrictive* default values for security attributes that are used to enforce the SFP.

Application Note: On start-up, one and only one attached COMPUTER shall be selected.

2 The TSF shall allow the *none* to specify alternative initial values to override the default values when an object or information is created.

5.1.3 Protection of the TOE Security Functions (FPT)

5.1.3.1 **FPT_RVM.1** (Non-bypassability of the TSP)

[No dependencies]

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

5.1.3.2 **FPT_SEP.1** (TSF Domain Separation)

[No dependencies]

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

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

5.1.4 Extended Requirements (EXT)

5.1.4.1 **EXT_VIR.1** (Visual Indication Rule)

[No dependencies]

1 A visual method of indicating which COMPUTER is CONNECTED to the shared set of PERIPHERAL DEVICES shall be provided.

Application Note: Does not *require* tactile indicators, but does not preclude their presence. The indication shall persist for the duration of the CONNECTION.

5.2 Target of Evaluation Security Assurance Requirements

Assurance requirement components are those of Evaluation Assurance Level 4 (EAL 4; *Methodically Designed, Tested, and Reviewe*d).

EAL 4 was selected because it challenges vendors to use best (rather than average) commercial practices, permits economically feasible retrofit of security-enhancing techniques, and avoids the non-trivial expense and rigor of formal methods.

The following requirements are identically those of Common Criteria EAL 4.

5.2.1 Configuration Management (ACM)

5.2.1.1 **ACM_AUT.1** (Partial CM Automation) [Dependencies: ACM_CAP.3]

1D The developer shall use a CM system.

2D The developer shall provide a CM plan.

1C The CM system shall provide an automated means by which only authorised changes are made to the TOE implementation representation.

2C The CM system shall provide an automated means to support the generation of the TOE.

3C The CM plan shall describe the automated tools used in the CM system.

4C The CM plan shall describe how the automated tools are used in the CM system.

1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.1.2 **ACM_CAP.4** (Generation Support and Acceptance Procedures) [Dependencies: ACM_SCP.1 and ALC_DVS.1]

1D The developer shall provide a reference for the TOE.

2D The developer shall use a CM system.

3D The developer shall provide CM documentation.

1C The reference for the TOE shall be unique to each version of the TOE.

2C The TOE shall be labelled with its reference.

3C The CM documentation shall include a configuration list, a CM plan, and an acceptance plan.

4C The configuration list shall describe the configuration items that comprise the TOE.

5C The CM documentation shall describe the method used to uniquely identify the configuration items.

6C The CM system shall uniquely identify all configuration items.

7C The CM plan shall describe how the CM system is used.

8C The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.

9C The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.

10C The CM system shall provide measures such that only authorised changes are made to the configuration items.

11C The CM system shall support the generation of the TOE.

12C The acceptance plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.

1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.1.3 **ACM_SCP.2** (Problem Tracking CM Coverage) [Dependencies: ACM_CAP.3]

1D The developer shall provide CM documentation.

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.

2C The CM documentation shall describe how configuration items are tracked by the CM system.

1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.2 Delivery and Operation (ADO)

5.2.2.1 **ADO_DEL.2** (Detection of Modification)
[Dependencies: ACM_CAP.3]

1D The developer shall document procedures for delivery of the TOE or parts of it to the user.

2D The developer shall use the delivery procedures.

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.

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.

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.

1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.2.2 **ADO_IGS.1**
(Installation, Generation, and Start-up Procedures)
[Dependencies: AGD_ADM.1]

1D The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

1C The documentation shall describe the steps necessary for secure installation, generation, and start-up of the TOE.

1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

2E The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

5.2.3 Development (ADV)

5.2.3.1 **ADV_FSP.2** (Fully Defined External Interfaces) [Dependencies: ADV_RCR.1]

1D The developer shall provide a functional specification.

1C The functional specification shall describe the TSF and its external interfaces using an informal style.

2C The functional specification shall be internally consistent.

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.

4C The functional specification shall completely represent the TSF.

5C The functional specification shall include rationale that the TSF is completely represented.

1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

5.2.3.2 **ADV_HLD.2** (Security Enforcing High-level Design)
[Dependencies: ADV_FSP.1 and ADV.RCR.1]

1D The developer shall provide the high-level design of the TSF.

1C The presentation of the high-level design shall be informal.

2C The high-level design shall be internally consistent.

3C The high-level shall describe the structure of the TSF in terms of subsystems.

4C The high-level design shall describe the security functionality provided by each subsystem of the TSF.

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.

6C The high-level design shall identify all interfaces to the subsystems of the TSF.

7C The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

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.

9C The high-level design shall describe the separation of the TOE into TSP-enforcing and other subsystems.

1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

2E The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

5.2.3.3 **ADV_IMP.1** (Subset of the Implementation of the TSF)
[Dependencies: ADV_LLD.1 and ADV_RCR.1 and ALC_TAT.1]

1D The developer shall provide the implementation representation for a selected subset of the TSF.

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.

2C The implementation representation shall be internally consistent.

1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

2E The evaluator shall determine that the least abstract TSF representation provided is an accurate and complete instantiation of the TOE security functional requirements.

5.2.3.4 **ADV_LLD.1** (Descriptive Low-level Design)
[Dependencies: ADV_HLD.2 and ADV_RCR.1]

1D The developer shall provide the low-level design of the TSF.

1C The presentation of the low-level design shall be informal.

2C The low-level design shall be internally consistent.

3C The low-level design shall describe the TSF in terms of modules.

4C The low-level design shall describe the purpose of each module.

5C The low-level design shall define the interrelationships between the modules in terms of provided security functionality and dependencies on other modules.

6C The low-level design shall describe how each TSP-enforcing function is provided.

7C The low-level design shall identify all interfaces to the modules of the TSF.

8C The low-level design shall identify which of the interfaces to the modules of the TSF are externally visible.

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.

10C The low-level design shall describe the separation of the TOE into TSP-enforcing and other modules.

1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

2E The evaluator shall determine that the low-level design is an accurate and complete instantiation of the TOE security functional requirements.

5.2.3.5 **ADV_RCR.1** (Informal Correspondence Demonstration) [No dependencies]

1D The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

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.

1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.3.6 **ADV_SPM.1** (Informal TOE Security Policy Model) [Dependencies: ADV_FSP.1]

1D The developer shall provide a TSP model.

2D The developer shall demonstrate correspondence between the functional specification and the TSP model.

1C The TSP model shall be informal.

2C The TSP model shall describe the rules and characteristics of all policies of the TSP that can be modeled.

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.

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.

1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.4 Guidance Documents (AGD)

5.2.4.1 **AGD_ADM.1** (Administrator Guidance)

[Dependencies: ADV_FSP.1]

1D The developer shall provide administrator guidance addressed to system administrative personnel.

1C The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

2C The administrator guidance shall describe how to administer the TOE in a secure manner.

3C The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

4C The administrator guidance shall describe all assumptions regarding user behaviour that are relevant to secure operation of the TOE.

5C The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

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.

7C The administrator guidance shall be consistent with all other documentation supplied for evaluation.

8C The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.

1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.4.2 **AGD_USR.1** (User Guidance)
[Dependencies: ADV_FSP.1]

1D The developer shall provide user guidance.

1C The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.

2C The user guidance shall describe the use of user-accessible security functions provided by the TOE.

3C The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.

4C The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behaviour found in the statement of TOE security environment.

5C The user guidance shall be consistent with all other documentation supplied for evaluation.

6C The user guidance shall describe all security requirements for the IT environment that are relevant to the user.

1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.5 Life Cycle Support (ALC)

5.2.5.1 **ALC_DVS.1** (Identification of Security Measures)

[No dependencies]

1D The developer shall produce development security documentation.

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.

2C The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.

1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

2E The evaluator shall confirm that the security measures are being applied.

5.2.5.2 **ALC_LCD.1** (Developer Defined Life-Cycle Model)
[No dependencies]

1D The developer shall establish a life-cycle model to be used in the development and maintenance of the TOE.

2D The developer shall provide life-cycle definition documentation.

1C The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.

2C The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.

1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.5.3 **ALC_TAT.1** (Well-Defined Development Tools)
[Dependencies: ADV_IMP.1]

1D The developer shall identify the development tools being used for the TOE.

2D The developer shall document the selected implementation-dependent options of the development tools.

1C All development tools used for implementation shall be well-defined.

2C The documentation of the development tools shall unambiguously define the meaning of all statements used in the implementation.

3C The documentation of the development tools shall unambiguously define the meaning of all implementation-dependent options.

1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.6 Tests (ATE)

5.2.6.1 **ATE_COV.2** (Analysis of Coverage)
[Dependencies: ADV_FSP.1 and ATE_FUN.1]

1D The developer shall provide an analysis of the test coverage.

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.

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.

1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.6.2 **ATE_DPT.1** (Testing: High-level Design)
[Dependencies: ADV_HLD.1 and ATE_FUN.1]

1D The developer shall provide the analysis of the depth of testing.

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.

1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.6.3 **ATE_FUN.1** (Functional Testing)
[No dependencies]

1D The developer shall test the TSF and document the results.

2D The developer shall provide test documentation.

1C The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.

2C The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.

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.

4C The expected test results shall show the anticipated outputs from a successful execution of the tests.

5C The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.

1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.6.4 **ATE_IND.2** (Independent Testing - Sample)
[Dependencies: ADV_FSP.1 and AGD_ADM.1 and AGD_USR.1 and ATE_FUN.1]

1D The developer shall provide the TOE for testing.

1C The TOE shall be suitable for testing.

2C The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

2E The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.

3E The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

5.2.7 Vulnerability Assessment (AVA)

5.2.7.1 **AVA_MSU.2** (Validation of Analysis)

[Dependencies: ADO_IGS.1 and ADV_FSP.1 and AGD_ADM.1 and AGD_USR.1]

1D The developer shall provide guidance documentation.

2D The developer shall document an analysis of the guidance documentation.

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.

2C The guidance documentation shall be complete, clear, consistent and reasonable.

3C The guidance documentation shall list all assumptions about the intended environment.

4C The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls).

5C The analysis documentation shall demonstrate that the guidance documentation is complete.

1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

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.

3E The evaluator shall determine that the use of the guidance documentation allows all insecure states to be detected.

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.

5.2.7.2 **AVA_SOF.1** (Strength of TOE Security Function Evaluation) [Dependencies: ADV_FSP.1 and ADV_HLD.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.

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.

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.

1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

2E The evaluator shall confirm that the strength claims are correct.

5.2.7.3 **AVA_VLA.2** (Independent Vulnerability Analysis) [Dependencies: ADV_FSP.1 and ADV_HLD.2 and ADV_IMP.1 and ADV_LLD.1 and AGD_ADM.1 and AGD_USR.1]

1D The developer shall perform and document an analysis of the TOE deliverables searching for ways in which a user can violate the TSP.

2D The developer shall document the disposition of identified vulnerabilities.

1C The documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

2C The documentation shall justify that the TOE, with the identified vulnerabilities, is resistant to obvious penetration attacks.

1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

2E The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure the identified vulnerabilities have been addressed.

3E The evaluator shall perform an independent vulnerability analysis.

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.

5E The evaluator shall determine that the TOE is resistant to penetration attacks performed by an attacker possessing a low attack potential.

6. Rationale

6.1 Security Objectives Rationale

All of the Security Objectives for the Environment are considered to be Secure Usage Assumptions.

O.CONF If the PERIPHERALS can be CONNECTED to more than one COMPUTER at any given instant, then a channel may exist which would allow transfer of information from one to the other. This is particularly important for DEVICES with bi-directional communications channels such as KEYBOARD and POINTING DEVICES.
Since many PERIPHERALS now have embedded microprocessors or microcontrollers, significant amounts of information may be transferred from one COMPUTER system to another, resulting in compromise of sensitive information. An example of this is transfer via the buffering mechanism in many KEYBOARDS.

Threats countered: T.PHYSICAL, T.RESIDUAL, T.STATE, T.TRANSFER

O.CONNECT The purpose of the TOE is to share a set of PERIPHERALS among multiple COMPUTERS. Information transferred to/from one SWITCHED COMPUTER is not to be shared with any other COMPUTER.

Threats countered: T.RESIDUAL, T.STATE, T.TRANSFER

O.INDICATE The USER must receive positive confirmation of SWITCHED COMPUTER selection.

Threats countered: T.SPOOF

O.INVOKE The TOE must be invoked whenever a switch selection is made.

Threats countered: T.BYPASS

O.NOPROG The functional capabilities of the TOE are finalized during manufacturing. The configuration of the TOE (operating parameters and other control information) may change.

Threats countered: T.LOGICAL, T.PHYSICAL

O.ROM Any software/firmware affecting the basic functionality of the TOE must be stored in a medium which prevents its modification.

Threats countered: T.LOGICAL, T.PHYSICAL

O.SELECT The USER must take positive action to select the current SWITCHED COMPUTER.

Threats countered: T.SPOOF

O.SWITCH The purpose of the TOE is to share a set of PERIPHERALS among multiple COMPUTERS. It makes no sense to have, for example, video CONNECTED to one COMPUTER while a POINTING DEVICE is CONNECTED to another COMPUTER.

Threats countered: T.TRANSFER

6.2 Security Requirements Rationale

None of the requirements imply probabilistic or permutational mechanisms; therefore, no strength of function claims are necessary.

FDP_ETC.1 (Export of User Data Without Security Attributes)

In typical TOE applications, USER data consists of HUMAN INTERFACE DEVICE control information. Also included is configuration information such as KEYBOARD settings that must be reestablished each time the TOE switches between COMPUTERS. These DEVICES neither expect nor require any security ATTRIBUTE information. The information content of the data passed through a CONNECTION is ignored.

Objectives addressed: O.CONF, O.CONNECT

FDP_IFC.1 (Subset Information Flow Control)

This captures the policy that no information flows between different PERIPHERAL PORT GROUP IDS.

This requirement is a dependency of FDP_ETC.1, FDP_IFF.1, FDP_ITC.1 and FMT_MSA.1.

Objectives addressed: O.CONF, O.CONNECT

FDP_IFF.1 (Simple Security Attributes)

This requirement identifies the security ATTRIBUTES needed to detail the operation of a switch and the rules allowing information transfer.

This requirement is a dependency of FDP_IFC.1.

Objectives addressed: O.CONF, O.CONNECT, O.SWITCH

FDP_ITC.1 (Import of User Data Without Security Attributes)

In typical TOE applications, USER data consists of HUMAN INTERFACE DEVICE control information. These DEVICES neither expect nor require any security ATTRIBUTE information.

Objectives addressed: O.CONF, O.CONNECT

FMT_MSA.1 (Management of Security Attributes)

This restricts the ability to change selected PERIPHERAL PORT GROUP IDS to the AUTHORIZED USER.

This requirement is a dependency of FMT_MSA.3.

Objectives addressed: O.SELECT

FMT_MSA.3 (Static Attribute Initialisation)

The TOE assumes a default PERIPHERAL PORT GROUP selection based on a physical switch position or a manufacturer's specified sequence for choosing among the CONNECTED COMPUTERS (CONNECTED here implies powered on).

This requirement is a dependency of FDP_IFF.1 and FDP_ITC.1.

Objectives addressed: O.SWITCH

FPT_RVM.1 (Non-bypassability of the TSP)

The Data Separation SFP must be enforced at all times during TOE operation. This requires that the TSP functions always be invoked.

Objectives addressed: O.INVOKE

FPT_SEP.1 (TSF Domain Separation)

The TSF needs to ensure that it protects itself against changes which might compromise its security functionality.

Objectives addressed: O.NOPROG, O.ROM

EXT_VIR.1 (Visual Indication Rule)

There must be some positive feedback from the TOE to the USER to indicate which SWITCHED COMPUTER is currently CONNECTED.

Part 2 of the Common Criteria does not provide a component appropriate to express the requirement for visual indication.

Objectives addressed: O.INDICATE

The set of security functional requirements can be partitioned into the following areas, analytically determined to be mutually exclusive and internally consistent:

Information Flow:	FDP_ETC.1 FDP_IFC.1 FDP_IFF.1 FDP_ITC.1
Group ID Management:	FMT_MSA.1 FMT_MSA.3 EXT_VIR.1
TSF Invocation and Isolation:	FPT_RVM.1 FPT_SEP.1

6.3 Dependencies Not Met

FMT_SMR.1 (Security Roles)

The TOE is not required to associate USERS with roles; hence, there is only one “role”, that of *USER*. This *deleted* requirement, a dependency of FMT_MSA.1 and FMT_MSA.3, allows the TOE to operate normally in the absence of *any* formal roles.

6.4 Mapping Tables

The indicated mappings do not necessarily imply that all aspects of the relations are resolved. For example, in Table 1, T.PHYSICAL is only partially addressed by O.NOPROG.

	O.CONF	O.CONNECT	O.INDICATE	O.INVOKE	O.NOPROG	O.ROM	O.SELECT	O.SWITCH		OE.MANAGE
T.BYPASS				X						
T.INSTALL										X
T.LOGICAL					X	X				
T.PHYSICAL	X				X	X				
T.RESIDUAL	X	X								
T.SPOOF			X				X			
T.STATE	X	X								
T.TRANSFER	X	X						X		

Table 1: Mapping of Threats to Objectives

Threats which are addressed by Security Objectives

	O.CONF	O.CONNECT	O.INDICATE	O.INVOKE	O.NOPROG	O.ROM	O.SELECT	O.SWITCH
FDP_ETC.1	X	X						
FDP_IFC.1	X	X						
FDP_IFF.1	X	X						X
FDP_ITC.1	X	X						
FMT_MSA.1							X	
FMT_MSA.3								X
FPT_RVM.1				X				
FPT_SEP.1					X	X		
EXT_VIR.1			X					

Table 2: Mapping of Security Functional Requirements to Objectives

Security Objectives which are addressed by Functional Requirements

Dependency	FDP_IFC.1	FDP_IFF.1	FDP_ITC.1		FMT_MSA.1	FMT_MSA.3	FMT_SMR.1
FDP_ETC.1	X						
FDP_IFC.1		X					
FDP_IFF.1	X					X	
FDP_ITC.1	X					X	
FMT_MSA.1	X						X
FMT_MSA.3					X		X
FPT_RVM.1							
FPT_SEP.1							
EXT_VIR.1							

Table 3: Mapping of Security Functional Requirements Dependencies

Terms of Reference

Attribute

(See Peripheral Port Group ID)

Authorized User

A USER who has been granted permission to interact with the TOE and all of its CONNECTED PERIPHERALS.

Computer

A programmable machine. The two principal characteristics of a computer are: it responds to a specific set of instructions in a well-defined manner, and It can execute a prerecorded list of instructions (a software program). For the purposes of this document, any electronic DEVICE controlling the MONITOR, and accepting signals from the KEYBOARD and POINTING DEVICE (if any) will qualify. Examples of computers under this definition are IBM-class personal computers (and so-called clones), desktop workstations, and control console INTERFACES into “mainframe” computers.

Connected

A state in which information can be intentionally transferred.

Connection

A path for information flow between two or more DEVICES.

Device

A unit of hardware, outside or inside the case or housing for the essential COMPUTER that is capable of providing INPUT to the essential COMPUTER or of receiving OUTPUT or both. The term PERIPHERAL is sometimes used as a synonym for device or any INPUT/OUTPUT unit.

Group

(See Peripheral Port Group)

Human Interface Devices

Those PERIPHERALS which primarily allow a USER to directly observe and/or modify the operation/status of a COMPUTER. Examples include a keyboard, video MONITOR, mouse, and an optical head tracker. Modems, printers, hard drives, and scanners are *not* such devices.

Input Device

Any machine that feeds data into a COMPUTER. This includes scanners, touch screens, and voice response systems.

Interface

The CONNECTION and interaction between hardware, software, and the USER.

Keyboard

A DEVICE which converts the physical action of a USER such as the depressing of one or more buttons into electronic signals corresponding to the bitwise symbol for a character in some form of electronic alphabet. The most common example is the type-writer-like keyboard found on most home COMPUTERS, but the definition also includes braille keypads among other DEVICES.

Monitor

A COMPUTER OUTPUT surface and projecting mechanism that show text and other graphic images from a COMPUTER system to a user, using a Cathode Ray Tube (CRT), Liquid Crystal Display (LCD), Light-Emitting Diode (LED), gas plasma, active matrix, or other image projection technology. The display (the terms *display* and *monitor* are often used interchangeably) is usually considered to include the screen or projection surface and the DEVICE that produces the information on the screen. In some COMPUTERS, the display is packaged in a separate unit called a monitor. Displays (and monitors) are also sometimes called Video Display Terminals (VDTs). Also included in this category are tac-tile braille OUTPUT DEVICES.

Object

(See Peripheral Data and State Information)

Output Device

Any machine capable of representing information from a COMPUTER. This includes display screens, printers, plotters, and synthesizers.

Peripheral

A DEVICE which is logically and electrically (or electromagnetically) CONNECTED to a COMPUTER, but normally mounted outside of the COMPUTER enclosure. MONITORS, KEYBOARDS, and POINTING DEVICES are all peripherals.

Peripheral Data

Information, including [buffered] STATE INFORMATION, sent from or to a PERIPHERAL.

Peripheral Port Group ("Group")/
Peripheral Port Group ID

A collection of HUMAN INTERFACE DEVICE PORTS treated as a single entity by the SWITCH. There is one Group for the set of *SHARED* PERIPHERALS and one Group for each *SWITCHED* COMPUTER directly CONNECTED to the SWITCH. Each SWITCHED COMPUTER Group has a unique logical ID. The shared Group ID is the same as that of the SWITCHED COMPUTER Group currently selected by the SWITCH.

Pointing Device

A DEVICE which converts relative positioning motion from a human operator into positioning information on a MONITOR. Examples of Pointing Devices include a mouse, trackball, joystick, and touchpad.

Port

An external socket for plugging in communications lines and/or PERIPHERALS.

Residual Data

Any PERIPHERAL DATA stored in a SWITCH.

Shared Peripheral

(See Peripheral Port Group)

State Information

The current or last-known status, or condition, of a process, transaction, or setting. "Maintaining state" means keeping track of such data over time.

Subject

(See Peripheral Port Group)

Switch

A DEVICE permitting a single set of PERIPHERALS to be shared among two or more COMPUTERS. Synonymous with TOE in this document.

Switched Computer

(See Peripheral Port Group)

User

The human operator of the TOE.

Acronyms

CCIB	Common Criteria Implementation Board
CCIMB	Common Criteria Interpretations Management Board
CM	Configuration Management
CRT	Cathode Ray Tube
DAC	Discretionary Access Control
EAL	Evaluation Assurance Level
FCC	Federal Communications Commission
FFRDC	Federally Funded Research and Development Center
ID	Identification
IEC	International Electrotechnical Commission
ISO	International Standards Organization
ISSE	Information Systems Security Engineer[ing]
ISSO	Information Systems Security Organization
IT	Information Technology
KVM	Keyboard-Video-Mouse
LCD	Liquid Crystal Display
LED	Light-Emitting Diode
MAC	Mandatory Access Control
PP	Protection Profile
PSS	Peripheral Sharing Switch
SFP	Security Function Policy
ST	Security Target

TOE Target of Evaluation

TSC TSF Scope of Control

TSF TOE Security Functions

TSP TOE Security Policy

VDT Video Display Terminal

References

1. Common Criteria for Information Technology Security Evaluation,
   Version 2.0, CCIB-98-028 (ISO/IEC 15408:1998), May 1998;
   Version 2.1, CCIMB-99-031 (ISO/IEC 15408:1999), August 1999.

2. ISSE Analysis - Electronic Computer Peripheral Switches,
   NSA/V23, draft dated 12 March 1999.

   ISSE Analysis/Keyboard-Video-Mouse (KVM) Switches,
   NSA/V23, draft dated 5 August 1999.

3. Network Security Framework Forum
   (renamed the Information Assurance Framework Forum),
   http://www.nsff.org

4. Network Security Framework Robustness Strategy (Chapter 4.4), Release 1.1
   3 December 1998.

5. http://ourworld.compuserve.com/homepages/david_fletcher1/Fletcher2/encyclop.htm
   Over 10,000 computer terms and definitions.

6. http://www.pcwebopaedia.com
   Online encyclopedia and search engine.

7. http://www.whatis.com
   Computer-related term definitions.

8. Title 47 CFR, Chapter 1 (FCC), Part 15 (Radio Frequency Devices);
   http://www.fcc.gov/oet/info/rules/part15/part15-mar99.pdf