Cybex SwitchView SC Series Switches Security Target

Document Version 1.0

June 23, 2003

Prepared for:

Avocent Corporation
4991 Corporate Drive
Huntsville, Alabama, 35805-6201

Prepared by:

Computer Sciences Corporation
132 National Business Parkway
Annapolis Junction, MD 20701

Revisions to Document		
Date	**Version**	**Changes Made**
November 11, 2002	0.1	Original
February 13, 2003	0.2	Made changes in response to AVO_EDR_002
February 20, 2003	0.3	Inserted “Cybex” in name of product.
March 18, 2003	0.4	Updated to resolve issues in EDR_003
June 23, 2003	1.0	Final

Table of Contents

List of Tables

List of Figures

1 INTRODUCTION

1 This Chapter presents security target (ST) identification information and an overview of the ST. An ST document provides the basis for the evaluation of an information technology (IT) product or system (e.g., Target of Evaluation). An ST principally defines:

- A security problem expressed as a set of assumptions about the security aspects of the environment; a list of threats which the product is intended to counter; and any known rules with which the product must comply (in Chapter 3, Security Environment).
- A set of security objectives and a set of security requirements to address that problem (in Chapters 4 and 5, Security Objectives and IT Security Requirements, respectively).
- The IT security functions provided by the Target of Evaluation (TOE) that meet the set of requirements (in Chapter 6, TOE Summary Specification).

2 The structure and contents of this ST comply with the requirements specified in the Common Criteria (CC), Part 1, Annex C, and Part 3, Chapter 5.

1.1 ST and TOE Identification

3 This section provides information needed to identify and control this ST and its Target of Evaluation (TOE), the TOE Name. This ST targets an Evaluation Assurance Level (EAL) 4 level of assurance.

ST Title	Cybex SwitchView SC Series Switches Security Target
ST Version	0.4
Date	March 18, 2003
Authors	Computer Sciences Corporation, Common Criteria Testing Lab Avocent Corporation
TOE Identification:	Cybex SwitchView SC (4 port), Model 520-147-004, Cybex SwitchView SC (8 port), Model 520-319-003
CC Identification:	Common Criteria for Information Technology Security Evaluation, Version 2.1, August 1999
ST Evaluation:	Computer Sciences Corporation
Keywords	Device sharing, multi-way switch, peripheral switching, keyboard-video-monitor/mouse (KVM) switch

1.2 References

4 The following documentation was used to prepare this ST:

[CC_PART1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated August 1999, version 2.1, CCIMB-99-031.

[CC_PART2] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated August 1999, version 2.1, CCIMB-

99-032.

[CC_PART3] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated August 1999, version 2.1, CCIMB-99-033.

[CEM_PART1] Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and General Model, dated 1 November 1997, version 0.6.

[CEM_PART2] Common Methodology for Information Technology Security Evaluation – Part 2: Evaluation Methodology, dated August 1999, version 1.0.

[PSS_PP] *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.0, 8 August 2000

1.3 Conventions, Terminology, and Acronyms

5 This section identifies the formatting conventions used to convey additional information and terminology having specific meaning. It also defines the meanings of abbreviations and acronyms used throughout the remainder of the document.

1.3.1 Conventions

6 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. Selected presentation choices are discussed here to aid the Security Target reader.

7 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 is used to assign a specific value to an unspecified parameter, such as the length of a password. An assignment is indicated by showing the value in square brackets [assignment_value(s)].
- Iteration of a component is used when a component is repeated more than once with varying operations. Iterated components are given unique identifiers by an iteration number or name in parenthesis appended to the component and element identifiers.
- The refinement operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold text**.
- The selection operation is picking one or more items from a list in order to narrow the scope of a component element. Selections are denoted by *underlined italicized text.*

8 Plain *italicized text* is used for both official document titles and text meant to be emphasized more than plain text.

9 **Assumptions:** TOE security environment assumptions are given names beginning with "A." and are presented in alphabetical order. This prefix will be subscripted to reflect a given component for multi-component TOEs as required.

Examples:

- A.ADMIN – Assumption allocated to TOE as an entity.
- A_C.CONFIG – Assumption allocated to the Console component.

10 **Threats:** TOE security threats are given names beginning with "T." and are presented in alphabetical order. This prefix will be subscripted to reflect threats to a given component for multi-component TOEs as required.

Examples:

T.ATTACK_DATA – Threat to/countered by the TOE as an entity.

T_R.ATTACK_DATA – Threat to/countered by the "remote" component of the TOE.

11 **Policies:** TOE security environment policies are given names beginning with "P." and are presented in alphabetical order. This prefix will be subscripted to reflect a given component for multi-component TOEs as required.

Examples:

P.ACCOUNT – Policy supported by the TOE as an entity.

P_C.ACCOUNT – Policy supported by the "Console" component of the TOE.

12 **Objectives:** Security objectives for the TOE and for the environment are given names beginning with "O." and "OE." respectively, and are presented in alphabetical order. These prefixes will be subscripted to reflect a given component for multi-component TOEs as required.

Examples:

O.ADMIN – Objective for the TOE as an entity.

OE.AUTHORIZATION – Objective for the environment.

O_R.ADMIN – Objective of the "remote" component of the TOE.

1.3.2 Terminology

13 In the Common Criteria, many terms are defined in Section 2.3 of Part 1. The following terms are a subset of those definitions. They are listed here to aid the user of the Security Target.

User	Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.
Human user	Any person who interacts with the TOE.
External IT entity	Any IT product or system, untrusted or trusted, outside of the TOE that interacts with the TOE.
Role	A predefined set of rules establishing the allowed interactions between a user and the TOE.
Identity	A representation (e.g., a string) uniquely identifying an authorized user, which can either be the full or abbreviated name of that user or a pseudonym.
Authentication data	Information used to verify the claimed identity of a user.

Object	An entity within the TOE Security Function (TSF[1]) Scope of Control (TSC[2]) that contains or receives information and upon which subjects perform operations.
Subject	An entity within the TSC that causes operations to be performed.
Authorized User	A user who may, in accordance with the TOE Security Policy (TSP[3]), perform an operation.
Security Functional Components	Express security requirements intended to counter threats in the assumed operating environment of the TOE.

14 In addition to the above general definitions, this Security Target provides the following specialized definitions: Terminology is specific to this ST is given in "Terms of Reference," Page 38, *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.0, 8 August 2000.

1.3.3 Common Criteria Acronyms

15 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
FIPS PUB	Federal Information Processing Standard Publication
IT	Information Technology
PP	Protection Profile
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy

As defined in the CC, Part 1, version 2.1:

1 TSF - A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.

2 TSC - The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.

3 TSP – A set of rules that regulate how assets are managed, protected and distributed within a TOE.

1.3.4 ST Acronyms

16 The following abbreviations are used in this Security Target to help describe the TOE, and the IT environment.

IBM	International Business Machines, Inc.
LED	Light Emitting Diode
PC/AT	Personal Computer / Advanced Technology
PS/2	Personal System 2
VGA / SVGA	Video Graphics Array / Super Video Graphics Array

17 Acronyms specific to this ST, and the referenced PP are given in "Acronyms," Page 42, *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.0, 8 August 2000.

1.4 TOE Overview

18 The TOE is a device, hereinafter referred to as a "Peripheral Sharing Switch" (PSS), or simply "switch," that permits a single set of human interface devices, keyboard, video, mouse, to be shared among two or more computers. Users who access secure and unsecure networks from one set of peripherals can rely on the SwitchView SC series of switches' unique architecture to keep their private data completely separate and secure at all times. There is no software to install or boards to configure.

19 The SwitchView SC series of switches work with IBM PC/AT and PS/2 systems with support for VGA and SVGA video. PS/2 keyboard and PS/2 mouse peripherals are supported through the rear of the unit. With the SwitchView SC, Model 520-147-004, the user can cycle through the available computer channels vial the *Select* button on the front panel. With the SwitchView SC, Model 520-319-003, there is an additional *Select* button associated with each specific port.

20 A summary of the SwitchView SC series switches security features can be found in Section 2, TOE Description. A detailed description of the SwitchView SC series switches security features can be found in Section 6, TOE Summary Specification.

1.5 Common Criteria Conformance

21 The TOE, SwitchView SC (4 port), Model 520-147-004, SwitchView SC (8 port), Model 520-319-003 is Part 2 extended, and Part 3 conformant. The TOE is conformant to Evaluation Assurance Level (EAL) 4. Also, the TOE is conformant to the following PP, *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.0, 8 August 2000.

2 TOE DESCRIPTION

22 This Chapter provides context for the TOE evaluation by identifying the product type and describing the evaluated configuration.

2.1 Product Type

23 The TOE is a device, hereinafter referred to as a "Peripheral Sharing Switch" (PSS), or simply "switch," that permits a single set of human interface devices to be shared among two or more computers. Users who access secure and unsecure networks from one set of peripherals can rely on the SwitchView SC series of switches' unique architecture to keep their private data completely separate and secure at all times. There is no software to install or boards to configure.

24 The SwitchView SC series of switches work with IBM PC/AT and PS/2 systems with support for VGA and SVGA video. PS/2 keyboard and PS/2 mouse peripherals are supported through the rear of the unit. With the SwitchView SC, Model 520-147-004, the user can cycle through the available computer channels vial the *Select* button on the front panel. With the SwitchView SC, Model 520-319-003, there is a *Select* button associated with each specific port.

2.2 Physical Scope and Boundary

25 The following components comprise the TOE: the Cybex SwitchView SC (4 port), Model 520-147-004, and Cybex SwitchView SC (8 port), Model 520-319-003 (shown in Figure 1).

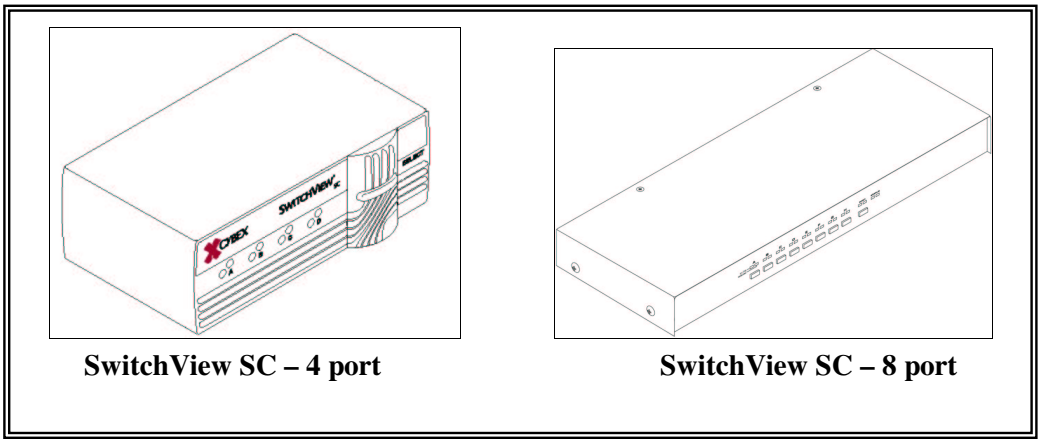

Figure 1: SwitchView SC Series Switches

26 The evaluated TOE configuration does not include any peripherals or computer components, including the cables or their associated connectors, attached to the TOE. The following figure depicts the TOE and its environment.

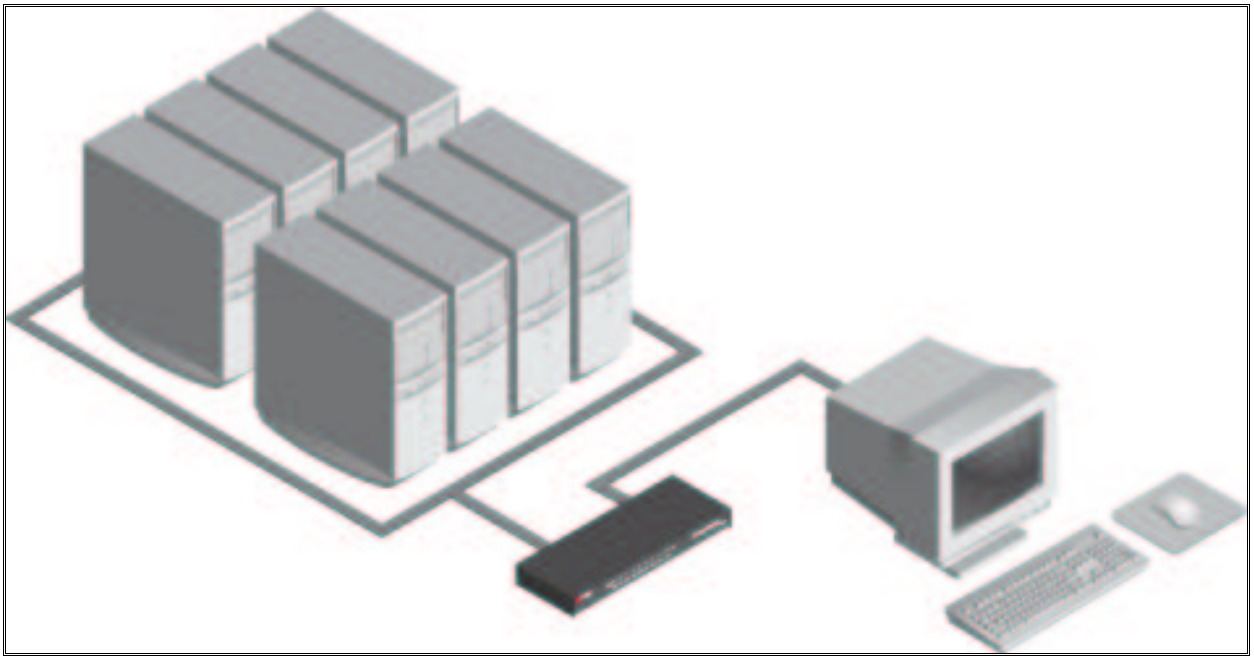

Figure 2: Depiction of TOE Deployment

2.3 Logical Scope and Boundary

27 The TOE logical scope and boundary consists of the security functions/features provided/controlled by the TOE.

28 The TOE provides the following security features:

- Data Separation (TSF_DSP), and
- Security Management (TSF_MGT)

29 In operation the TOE is not concerned with the user information flowing between the shared peripherals and the switched computers. It only provides a single logical connection between the shared peripheral group and the one selected computer (TSF_DSP).

30 The TOE allows for the connected computers to be powered-up all-at-once or one at a time. The green LEDs over each channel will light, indicating that the attached computer is powered on. To select or switch computers, the TOE provides a *select* switch, or switches in the case of the SwitchView SC (8 port), that allow(s) the human user to explicitly determine to which computer the shared set of peripherals is connected (TSF_MGT). This connection is visually displayed by an amber LED over the selected channel.

2.4 TOE Features Outside of Evaluation Scope

31 There are no TOE features outside the evaluation scope.

3 TOE SECURITY ENVIRONMENT

32 The assumptions and threat identification combined with any organization security policy statement or rules requiring TOE compliance provides the definition of the security environment. It is necessary that a comprehensive security policy be established for the site in which the product is operated and that it is enforced and adhered to by all users of the product. The security policy is expected to include measures for:

- ***Physical security*** - to restrict physical access to areas containing the product, computer system and associated equipment and protect physical resources, including media and hardcopy material, from unauthorized access, theft or deliberate damage.
- ***Procedural security*** - to control the use of the computer system, associated equipment, the product and information stored and processed by the product and the computer system, including use of the product's security features and physical handling of information.
- ***Personnel security*** - to limit a user's access to the product and to the computer system to those resources and information for which the user has a need-to-know and, as far as possible, to distribute security related responsibilities among different users.

3.1 Assumptions

33 The specific conditions listed in "Secure Usage Assumptions," Section 3.1, *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.0, 8 August 2000, are assumed to exist for the TOE.

3.2 Threats

34 Threats may be addressed either by the TOE or by its intended environment (for example, using personnel, physical, or administrative safeguards). These two classes of threats are discussed separately.

3.2.1 Threats Addressed by the TOE

35 "Threats to Security," Section 3.2, *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.0, 8 August 2000, identifies threats to the assets against which specific protection within the TOE is required.

3.2.2 Threats Addressed by the Operating Environment

36 *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.0, 8 August 2000, identifies no threats to the assets against which specific protection within the TOE environment is required.

3.3 Organizational Security Policies

37 *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.0, 8 August 2000, identifies no organization security policies (OSPs) to which the TOE must comply.

4 SECURITY OBJECTIVES

38 The purpose of the security objectives is to detail the planned response to a security problem or threat. Threats can be directed against the TOE or the security environment or both, therefore, the CC identifies two categories of security objectives:

- Security objectives for the TOE, and
- Security objectives for the Operating Environment.

4.1 SECURITY OBJECTIVES FOR THE TOE

39 "Security Objectives for the Target of Evaluation," Section 4.1, *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.0, 8 August 2000 identifies the security objectives to address security concerns that are directly addressed by the TOE.

4.2 SECURITY OBJECTIVES FOR THE ENVIRONMENT

40 "Security Objectives for the Environment," Section 4.2, *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.0, 8 August 2000, identifies security objectives to address security concerns that are directly addressed by the TOE environment.

5 IT SECURITY REQUIREMENTS

41 This section defines the IT security requirements that shall be satisfied by the TOE or its environment:

42 The CC divides TOE security requirements into two categories:

- Security functional requirements (SFRs) (such as, identification and authentication, security management, and user data protection) that the TOE and the supporting evidence need to satisfy to meet the security objectives of the TOE.
- Security assurance requirements (SARs) that provide grounds for confidence that the TOE and its supporting IT environment meet its security objectives (e.g., configuration management, testing, and vulnerability assessment).

43 These requirements are discussed separately within the following subsections.

5.1 TOE Security Functional Requirements

44 The TOE satisfies the SFRs delineated in "Target of Evaluation Security Requirements," Section 5.1, *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.0, 8 August 2000.

5.2 TOE Security Assurance Requirements

45 The security assurance components are specified in "Target of Evaluation Security Assurance Requirements," Section 5.2, *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.0, 8 August 2000

5.3 Security Requirements for the IT Environment

46 There are no security functional requirements for the IT Environment.

5.4 Explicitly Stated Requirements for the TOE

47 This ST does contain the explicitly stated requirement for the TOE as specified in "EXT_VIR.1 (Visual Indication Rule)," Section 5.1.4.1, *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.0, 8 August 2000.

5.5 SFRs With SOF Declarations

48 The overall Strength of Function (SOF) claim for the TOE is SOF-medium (Reference "Threats to Security," Section 3.2, *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.0, 8 August 2000.

6 TOE SUMMARY SPECIFICATION

49 This section presents an overview of the security functions implemented by the TOE and the Assurance Measures applied to ensure their correct implementation.

6.1 TOE Security Functions

50 This section presents the security functions performed by the TOE to satisfy the identified SFRs in Section 5.1.1. Traceability to SFRs is also provided.

6.1.1 Data Separation (TSF_DSP)

51 In operation the TOE is not concerned with the content of user information flowing between the shared peripherals and the switched computers. It only provides a single logical connection between the shared peripheral group and the one selected computer supporting the Data Separation Security Functional Policy – "the TOE shall allow peripheral data and state information to be transferred only between peripheral port groups with the same ID." The TOE interfaces ensure that confidentiality of information is not violated by isolating signals electrically and through firmware modules that ensure that information is passed only between the user peripherals and the selected computer.

52 The TOE does not have software to install, or boards to configure. The logic contained within the TOE is protected from unauthorized modification through the use of discrete components.

53 **FUNCTIONAL REQUIREMENTS SATISFIED:** FDP_ETC.1, FDP_IFC.1, FDP_IFF.1, FDP_ITC.1, FPT_RVM.1, FPT_SEP.1

6.1.2 Security Management (TSF_MGT)

54 The TOE allows for the connected computers to be powered-up all-at-once or one at a time. The green LEDs over each channel will light, indicating that the attached computer is powered on. To select or switch computers, the TOE provides a *select* switch, and in the case of the SwitchView SC (8 port) port-specific switches, that allow(s) the human user to explicitly determine to which computer the shared set of peripherals is connected. This connection is visually displayed by an amber LED over the selected channel.

55 **FUNCTIONAL REQUIREMENTS SATISFIED:** FMT_MSA.1, FMT_MSA.3, EXT_VIR.1

6.2 Assurance Measures

56 The TOE satisfies the CC EAL 4 assurance requirements as specified in "Target of Evaluation Security Assurance Requirements" Section 5.2, *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.0, 8 August 2000.

57 Per the conformance statement provided in Section 1.5 of this ST, the evidence requirements will be met with respect to presentation and content as specified in [CC_PART3] for each of the assurance requirements claimed.

7 PROTECTION PROFILE (PP) CLAIMS

58 This ST claims compliance for the following PP:

Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile, Version 1.0, 8 August 2000

59 As specified in Section 5 of this ST, the security requirements are referred back to the PP that this ST is claiming compliance with, and there were no operations performed on those requirements statements in the PP by this ST.

60 As specified in Section 4 of this ST, the security objectives are referred back to the PP that this ST is claiming compliance with, and there are no additional objectives. As specified in Section 5 of this ST, the security requirements are referred back to the PP that this ST is claiming compliance with and there are no additional IT security requirements.

8 RATIONALE

61 This section demonstrates the completeness and consistency of this ST by providing justification for the following:

Traceability The security objectives for the TOE and its environment are explained in terms of threats countered and assumptions met. The SFRs are explained in terms of objectives met by the requirement. The traceability is illustrated through matrices that map the following:

- security objectives to threats encountered
- environmental objectives to assumptions met
- SFRs to objectives met

Assurance Level A justification is provided for selecting an EAL 4 level of assurance for this ST.

SOF A rationale is provided for the SOF level chosen for this ST.

Dependencies A mapping is provided as evidence that all dependencies are met.

8.1 Security Objectives Rationale

62 This section demonstrates that all security objectives for the TOE are traced back to aspects of the identified threats to be countered and/or aspects of the organizational security policies to be met by the TOE.

63 This ST claims conformance to the *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.0, without additional objectives. Consequently the security objectives rationale is provide in Section 6, *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.0, 8 August 2000, and are claimed to be adequate for this ST.

8.2 Security Requirements Rationale

64 This section provides evidence that demonstrates that the security objectives for the TOE and the IT environment are satisfied by the security requirements.

65 This ST claims conformance to the *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.0, without additional security requirements and without any operations performed on the IT security requirements specified in the cited PP. Consequently the security requirements rationale is provide in Section 6, *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.0, 8 August 2000, and are claimed to be adequate for this ST.

8.3 Rationale For Assurance Level

66 This ST claims conformance to the *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.0. In this PP, the TOE environment is described as being exposed to a moderate level of risk (Reference Section 3.2, *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.0, 8 August 2000). As such, the Evaluation Assurance Level 4 is appropriate.

8.4 Rationale For TOE Summary Specification

67 This section demonstrates that the TSFs and Assurance Measures meet the SFRs.

68 The specified TSFs work together to satisfy the TOE SFRs. The following table provides a mapping of SFRs to the TSFs to show that each SFR is captured within a security function.

Table 1: SFR to TSF Mapping

SFR	Name	TSF	Name
FDP_ETC.1	Export of User Data Without Security Attributes	TSF_DSP	Data Separation
FDP_IFC.1	Subset Information Flow Control	TSF_DSP	Data Separation
FPD_IFF.1	Simple Security Attributes	TSF_DSP	Data Separation
FDP_ITC.1	Import of User Data Without Security Attributes	TSF_DSP	Data Separation
FMT_MSA.1	Management of Security Attributes	TSF_MGT	Security Management
FMT_MSA.3	Static Attribute Initialization	TSF_MGT	Security Management
FPT_RVM.1	Non-bypassability of the TSP	TSF_DSP	Data Separation
FPT_SEP.1	TSF Domain Separation	TSF_DSP	Data Separation
EXT_VIR.1	Visual Indication Rule	TSF_MGT	Security Management

8.4.1 TOE Assurance Requirements

69 Section 6.2 of this document identifies the Assurance Measures implemented by Avocent to satisfy the assurance requirements of EAL 4 as delineated in the table in Annex B of the CC, Part 3, and Section 5.2, *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.0, 8 August 2000.

8.4.2 TOE SOF Claims

70 The overall TOE SOF claim is SOF-medium because this SOF is sufficient to resist the threats identified in Section 3.2. Section 8.1 provides evidence that demonstrates that TOE threats are countered by the TOE security objectives. Sections 8.2.1 and 8.2.2 demonstrate that the security objectives for the TOE are satisfied by the security requirements. The SOF-medium claim for the TOE applies because the TOE protects against an attacker of average expertise, with few resources, and moderate motivation. The claim of SOF-medium ensures that the mechanism is resistant to a moderate attack potential.

8.5 Rationale For SFR and SAR Dependencies

71 This ST claims conformance to the *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.0, the rationale with respect to SFR and SAR dependencies is given in Sections 6.2 and 6.3 of the referenced PP.

8.6 Rationale for Explicitly Stated Requirements

72 By claiming conformance to the *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.0, this ST contains an explicitly stated requirement. The rationale for this requirement is given in Section 6.2 of the referenced PP.

8.7 Internal Consistency and Mutually Supportive Rationale

73 The set of security requirements provided in this ST form a mutually supportive and internally consistent whole for the following reasons:

a) The choice of security requirements is justified as shown in Sections 8.3 and 8.4. The choice of SFRs and SARs is based on the assumptions about the objectives for, and the threats to, the TOE and the security environment. This ST provides evidence that the security objectives counter threats to the TOE, and that physical, personnel, and procedural assumptions are satisfied by security objectives for the TOE environment.

b) The security functions of the TOE satisfy the SFRs as shown in Section 8.4. All SFR and SAR dependencies have been satisfied or rationalized as shown in Section 8.5 and described in Section 8.6.

c) The SARs are appropriate for the assurance level of EAL 4 and are satisfied by the TOE as shown in Section 8.4.1. EAL 4 was chosen to provide a medium level of independently assured security with the assumption that products used in these environments will meet the security needs of the environment.

d) The SFRs and SARs presented in Section 5 and justified in Sections 8.3 and 8.4 are internally consistent. There is no conflict between security functions, as described in Section 2 and Section 6, and the SARs to prevent satisfaction of all SFRs.