National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

Avocent Cybex SwitchView SC Series SC620, SC640, and SC740

Report Number: CCEVS-VR-10450-2011

Dated: 6 June 2011

Version: 1.0

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

Department of Defense
National Security Agency
9800 Savage Road
Fort Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

Brad O'Neil

Mitre Corporation

Franklin Haskell

Mitre Corporation

Common Criteria Testing Laboratory

Gregory Bluher

Computer Sciences Corporation

1. EXECUTIVE SUMMARY

This report is intended to assist the end-user of this product and any security certification Agent for the end-user with determining the suitability of this Information Technology (IT) product in their environment. End-users should review both the Security Target (ST), which is where specific security claims are made, in conjunction with this Validation Report (VR), which describes how those security claims were evaluated.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Avocent Cybex SwitchView SC Series SC620, SC640, and SC740. The evaluation was performed by Computer Sciences Corporation (CSC) Common Criteria Testing Laboratory (CCTL) and was complete in June 2011. The evaluation was performed to conform to the requirements of the Common Criteria for Information Technology Security Evaluation (CC), Version 3.1, Revision 2, dated September 2007, and the Common Evaluation Methodology for IT Security Evaluation (CEM), Version 3.1, Revision 2, dated September 2007.

The information in this report is largely derived from the Security Target (ST), Evaluation Technical Report (ETR) and associated test report. The ST was written by Avocent Corporation. The ETR and Team Test Report used in developing this validation report were written by CSC. The evaluation team determined the product to be Part 2 extended and Part 3 conformant, and meets the assurance requirements of EAL 2 augmented with ALC_FLR.2. The product also meets demonstrable compliance with the *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile, Version 2.1,* dated September 7, 2010.

The Target of Evaluation (TOE) is a peripheral sharing switch (PSS) that permits a single set of human interface devices: DVI-I video, Audio (input and output), USB keyboard, and USB mouse to be shared among two or more computers. Each switch has a "select" button associated with each specific computer port. For the convenience of the operator, these models have USB ports on the rear of the device. There is no software to install or boards to configure.

The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site (www.niap.ccevs.org). The report presents the evaluation results, their justifications, and the conformance results. This report is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied.

Table 1: TOE Models and Features

Model	TOE Identification Part Numbers	Ports	Interfaces
Avocent Cybex	520-866-501	2	Single-head, Dual-link DVI-I,

SwitchView SC620			Audio (input and output), USB keyboard, and USB mouse
Avocent Cybex SwitchView SC640	520-869-501	4	Single-head, Dual-link DVI-I, Audio (input and output), USB keyboard, and USB mouse
Avocent Cybex SwitchView SC740	520-868-501	4	Dual-head, Dual-link DVI-I, Audio (input and output), USB keyboard, and USB mouse

In its evaluated configuration, the TOE is connected to one or more computers and shared peripherals as described in the User Guidance delivered with the TOE.

1.1. Interpretations

The Evaluation Team performed an analysis of the international interpretations of the CC and the CEM and determined that none of the international interpretations issued by the Common Criteria Interpretations Management Board (CCIMB) were applicable to this evaluation.

The TOE is also compliant with all International interpretations with effective dates on or before November 15, 2010.

2. IDENTIFICATION

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

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

Table 2 provides information needed to completely identify the product, including:

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

Table 2: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Target of Evaluation	Avocent Cybex SwitchView SC Series SC620, SC640, and SC740
Protection Profile	*Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile, Version 2.1,* dated September 7, 2010
Security Target	Avocent Cybex SwitchView SC Series Switches Security Target, Version 6.0, dated April 19, 2011
Dates of evaluation	December 2010 through June 2011
Evaluation Technical Report	*Evaluation Technical Report for a Target of Evaluation for the Avocent SwitchView SC Series: SC620, SC640, and SC740 Switches, Version 1.0, May 4, 2011*
Conformance Result	Part 2 extended and Part 3 EAL 2 augmented with ALC_FLR.2
Common Criteria version	Common Criteria for Information Technology Security Evaluation Version 3.1, Revision 2, September 2007
Common Evaluation Methodology (CEM) version	CEM version 3.1R2, September 2007
Sponsor	Avocent Corporation
Developer	Avocent Corporation
Evaluators	Gregory Bluher of Computer Sciences Corporation

3. SECURITY POLICY

The TOE enforces the following security policies:

3.1. Data Separation Policy

The TOE implements the Data Separation Security Function Policy (SFP) as outlined in Section 2 of Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile, Version 2.1, dated September 7, 2010.

Signals processed by the TOE are shared peripheral device data, Data Display Channel information, and video signals. Specific versions of the TOE accommodate subsets of the listed signals to support popular types of computers. In all cases, the TOE ensures data separation for all signal paths using both hardware and firmware.

The basic arrangement of the microprocessors used for shared peripheral data ensures data separation in hardware by physical separation of the microprocessors connected to the user's peripheral devices from the microprocessors connected to the attached computers. In operation, the main processor moves data received from the shared peripherals to the microprocessor corresponding to the selected computer. The processor dedicated to the selected computer sends data to the computer. Separation is ensured in hardware by use of separate microprocessors for each of the computers and for the shared user peripheral devices.

Separation in firmware is ensured by firmware design consisting of dedicated functions and static memory assignment with no third-party library functions or multitasking executives.

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.

Shared peripheral status for each computer is stored by the processor associated with each computer. 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.

3.2. Security Management Policy

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 port-specific switches that allow 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. The TOE also provides the TOE user with the management function of modifying the PERIPHERAL PORT GROUP IDs.

4. ASSUMPTIONS

4.1. Physical Security Assumptions

A key environmental assumption is physical security, for it is assumed appropriate physical security protection will be applied to the TOE hardware commensurate with the value of the IT assets. Specifically, the TOE is assumed to be located within a facility providing controlled (i.e., employee-only) access to prevent unauthorized physical access to internal parts of the TOE.

4.2. Personnel Security Assumptions

It is assumed that an authorized user possesses the necessary privileges to access the information transferred by the TOE – users are authorized users. It is also assumed that the TOE is installed and managed in accordance with the manufacturer's directions. It is assumed that the authorized user is non-hostile and follows all usage guidance.

4.3. Threats Addressed by the TOE

This section identifies the threats addressed by the TOE. 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.INVALIDUSB	The AUTHORIZED USER will connect unauthorized USB devices to the peripheral switch.
T.RESIDUAL	RESIDUAL DATA may be transferred between PERIPHERAL PORT GROUPS with different IDs.
T.ROM_PROG	The TSF may be modified by an attacker such that code embedded in reprogrammable ROMs is overwritten, thus leading to a compromise of the separation-enforcing components of the code and subsequent compromise of the data flowing through the TOE.
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.TRANSFER	A CONNECTION, via the TOE, between COMPUTERS may allow information transfer.

4.4. Threats Addressed by the Operating Environment

Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile, Version 2.1, dated September 7, 2010, identifies no threats to the assets against which specific protection within the TOE environment is required.

4.5. Organizational Security Policies

Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile, Version 2.1, dated September 7, 2010, identifies no organization security policies (OSPs) to which the TOE must comply.

5. ARCHITECTURAL INFORMATION

5.1. Logical Scope and Boundary

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

The TOE provides the following security features:

- Data Separation (TSF_DSP), and
- Security Management (TSF_MGT)
- Invalid USB Connection (TSF_IUC)
- Read-only ROMs (TSF_ROM)

Data Separation (TSF_DSP)

The TOE implements the Data Separation Security Function Policy (SFP) as outlined in Section 2 of *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 2.1, dated September 7, 2010. 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).

Security Management (TSF_MGT)

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 *select* switches, that allow 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.

Invalid USB Connection (TSF_IUC)

All USB devices connected to the Peripheral switch are interrogated to ensure that they are valid (pointing device and keyboard). No further interaction with non-valid devices is allowed to be performed.

Read-only ROMs (TSF_ROM)

TSF software embedded in TSF ROMs is contained in one-time-programmable read-only memory permanently attached (non-socketed) to a circuit assembly.

5.2. Physical Scope and Boundary

The TOE is a peripheral sharing switch. The physical boundary of the TOE consists of one Avocent Cybex SwitchView switch (see **Error! Reference source not found.**), and its accompanying User and Administrator Guidance, listed as below:

- QUICK INSTALLATION GUIDE SwitchView™ SC620/640 2/4-Port DVI-I/USB Switches with Audio (590-1050-501A)

- QUICK INSTALLATION GUIDE SwitchView™ SC740 4-Port, Dual-Head DVI-I/USB Switch with Audio (590-1051-501A)

In its evaluated configuration, the TOE is connected to one or more computers and shared peripherals as described in the User Guidance delivered with the TOE.

The following figure depicts the TOE and its environment.

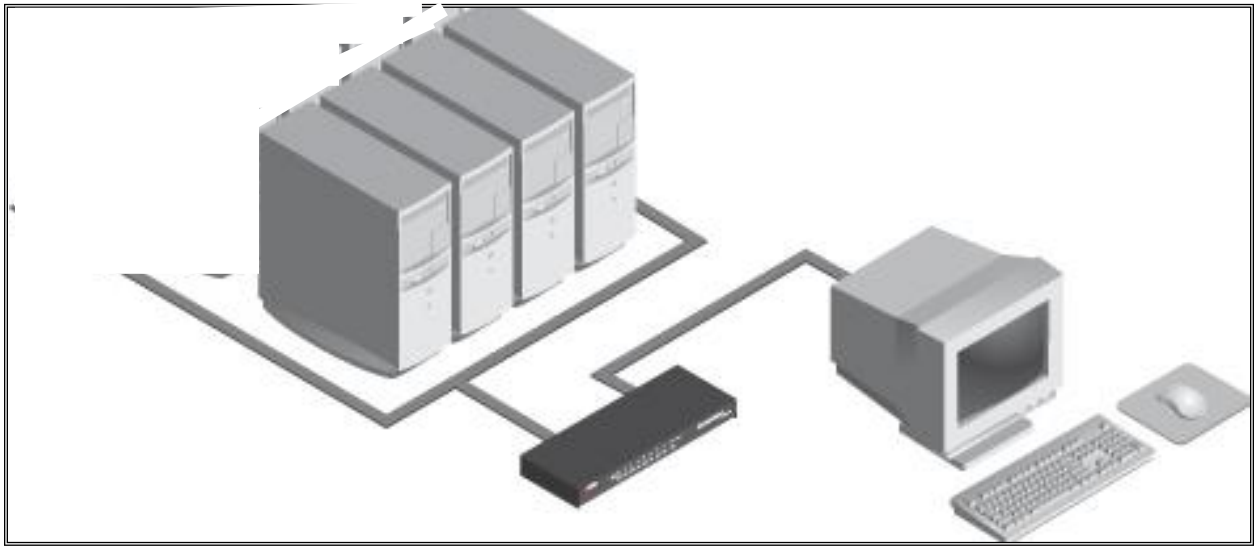


Figure 1: Depiction of TOE Deployment

6. DOCUMENTATION

This section details the documentation that is (a) delivered to the customer, and (b) was used as evidence for the evaluation of the Avocent Cybex SwitchView SC Series SC620, SC640, and SC740. Note that not all evidence is available to customers. The following documentation is available to the customer:

- QUICK INSTALLATION GUIDE SwitchView™ SC620/640 2/4-Port DVI-I/USB Switches with Audio (590-1050-501A)
- QUICK INSTALLATION GUIDE SwitchView™ SC740 4-Port, Dual-Head DVI-I/USB Switch with Audio (590-1051-501A)

The remaining evaluation evidence is described in the Evaluation Technical Report developed by Computer Sciences Corporation.

7. IT PRODUCT TESTING

This section describes the testing efforts of the Developer and the evaluation team.

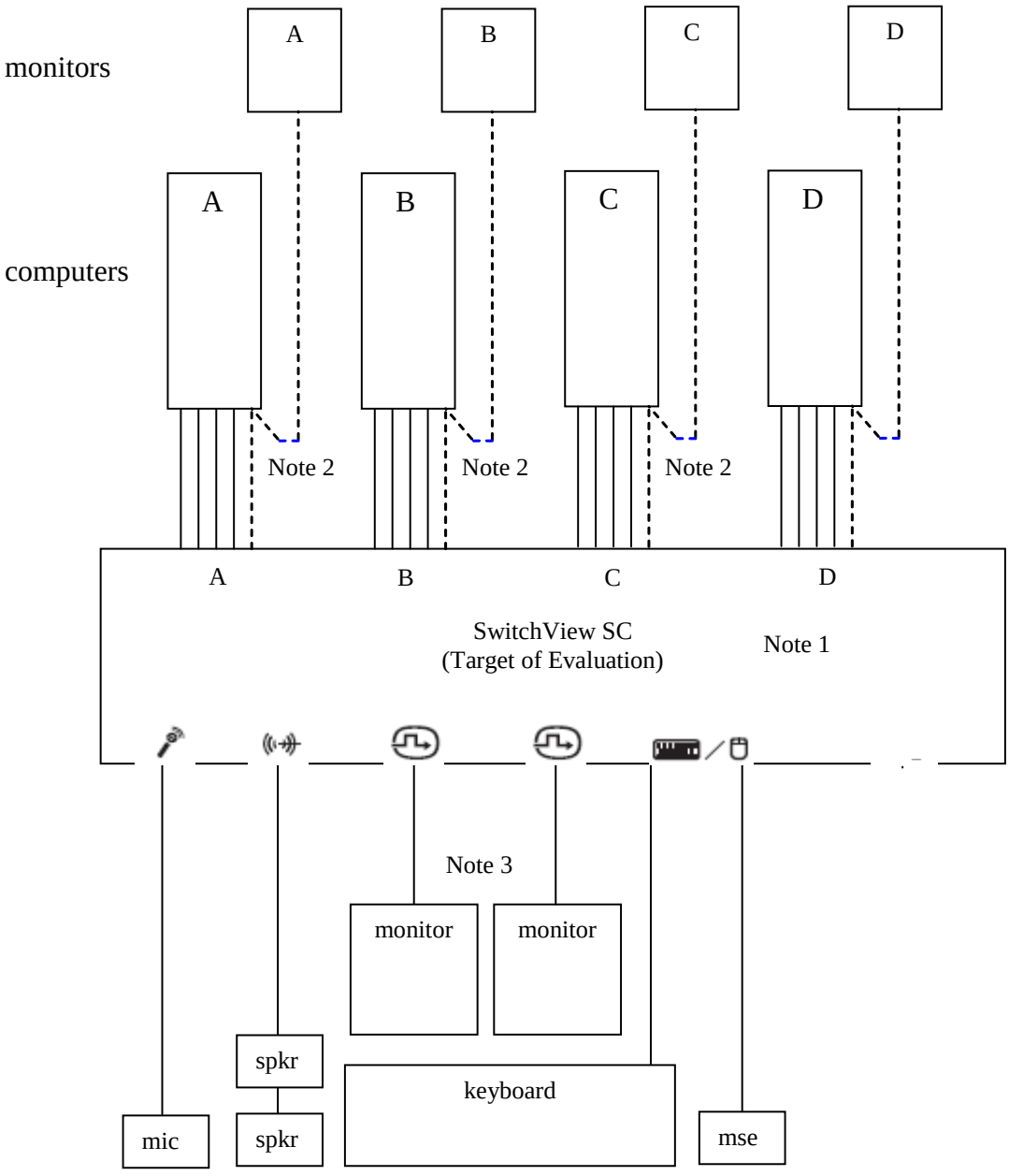
7.1. Developer testing

Test procedures were written by the Developer and designed to be conducted using manual interaction with the TOE interfaces. The developer tested all of the interfaces to the TOE and in doing so tested all TSFs.

The Developer tested the TOE consistent with the Common Criteria evaluated configuration identified in the ST. The Developer's approach to testing is defined in the TOE Test Plan. The expected and actual test results (ATRs) are also included with each of the tests in the TOE Test Procedures. Each test case was assigned an identifier that was used to reference it throughout the testing evidence.

The evaluation team analyzed the Developer's testing to ensure adequate coverage for EAL 2. The evaluation team determined that the Developer's actual test results matched the Developer's expected test results.

The following diagram depicts the test environment that was used by the Developers. The Evaluators assessed that the test environment used by the Developers was appropriate and mirrored this test configuration during Independent testing.



Notes:

1. Four-port TOE set-up is illustrated. Omit computers C and D with two-port TOE.

2. Connect computer video directly to monitors where dictated by test procedure, otherwise connect computer video to TOE. It is also acceptable to use a single monitor, moving it from computer to computer during the test.

3. Dual-video model is illustrated. Omit one monitor for single-video models: SC620 and SC640.

7.2. Evaluation team independent testing

The evaluation team conducted independent testing both at the CCTL and the Developer's facilities. For the testing at the CCTL, the TOE was delivered by common carrier, FedEx, and a signature receipt was required. The evaluation team installed and configured the TOE according to vendor installation instructions and the evaluated configuration as identified in the Security Target.

The evaluation team confirmed the technical accuracy of the setup and installation guide during installation of the TOE while performing work unit ATE_IND.2. The evaluation team confirmed that the TOE version delivered for testing was identical to the version identified in the ST.

The evaluation team used the Developer's Test Plan as a basis for creating the Independent Test Plan. The evaluation team analyzed the Developer's test procedures to determine their relevance and adequacy to test the security function under test. The following items represent a subset of the factors considered in selecting the functional tests to be conducted:

- Security functions that implement critical security features
- Security functions critical to the TOE's security objectives
- Security functions that gave rise to suspicion regarding the behavior of the security features during the documentation evidence evaluation
- Security functions not tested adequately in the vendor's test plan and procedures

The evaluation team repeated all of the Sponsor's test cases and designed additional independent tests. The additional test coverage was determined based on the analysis of the Developer test coverage and the ST.

The evaluators examined the ADV evidence listed in Section 1.2 above and elected to run the developer's tests for all three models under evaluation.

Each TOE Security Function was exercised at least once, and the evaluation team verified that each test passed.

7.3. Vulnerability analysis

The evaluation team gained assurance that the TOE does not contain exploitable flaws or weaknesses in the TOE based on the evaluation team's Vulnerability Analysis.

The Developer performed a Vulnerability Analysis of the TOE to identify any obvious vulnerability in the product and to show that it is not exploitable in the intended environment for the TOE operation. In addition, the evaluation team conducted a search of the public vulnerability sites to determine the thoroughness of the analysis.

Based on the results of the team's Vulnerability Analysis and an in-depth analysis (to the code level in several instances) of the TOE design evidence, the evaluation team came to the conclusion that obvious penetration attempts are not possible through the TOE external interfaces. As indicated in the design documentation, direct access to the TOE security functions is not possible without disassembly of the TOE, thus penetration is not

possible via the product control, i.e., user/administrator interfaces. Additionally, no configuration items are provided for the security functionality of the TOE thus it cannot be configured in an insecure state. The security functionality is inherent in the design and internal functioning of the TOE.

8. EVALUATED CONFIGURATION

The evaluated configuration as defined in the Security Target, consists of one Avocent Cybex SwitchView switch (see **Error! Reference source not found.**).

The Avocent Cybex SwitchView SC Series SC620, SC640, and SC740 must be configured in accordance with the following Guidance Documents:

- QUICK INSTALLATION GUIDE SwitchView™ SC620/640 2/4-Port DVI-I/USB Switches with Audio (590-1050-501A)
- QUICK INSTALLATION GUIDE SwitchView™ SC740 4-Port, Dual-Head DVI-I/USB Switch with Audio (590-1051-501A)

9. RESULTS OF THE EVALUATION

The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) processes and procedures. The TOE was evaluated against the criteria contained in the Common Criteria for Information Technology Security Evaluation, Version 3.1R2. The evaluation methodology used by the evaluation team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 3.1R2.

Computer Sciences Corporation (CSC) has determined that the product meets the security criteria in the Security Target, which specifies an assurance level of EAL 2 augmented with ALC_FLR.2. A team of Validators, on behalf of the CCEVS Validation Body, monitored the evaluation. The evaluation effort was finished on May 4, 2011. A final Validation Oversight Review (VOR) was held on June 3, 2011 and final changes to the VR were completed on June 7, 2011.

10. VALIDATOR COMMENTS

Potential customers should note that Common Access Card readers are not included as allowable devices in the Peripheral Sharing Switch Protection Profile at the present time. This product was built to conform to that PP and therefore does not support CAC readers. Indeed, any product claiming conformance to the current PSS PP cannot allow such devices. Parties needing this functionality must buy a different product. Avocent does have these in its product line. The next version of the PP may include CAC readers as allowable devices.

11. ANNEXES

None

12. SECURITY TARGET

Avocent Cybex SwitchView SC Series Switches Security Target, Version 6.0, dated April 19, 2011

13. GLOSSARY

- **Administrator:** Role applied to user with full access to all aspects of the Cybex SwitchView SC Series Switches.
- **Attack:** An attack is an exploited threat or an attempt to bypass security controls on a computer. The attack may alter, release, or deny data. Whether an attack will succeed depends on the vulnerability of the computer system and the effectiveness of existing countermeasures.
- **Common Criteria Testing Laboratory (CCTL):** An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Evaluation:** The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence:** Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Target of Evaluation (TOE):** A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Threat:** Means through which the ability or intent of a threat agent to adversely affect the primary functionality of the TOE, facility that contains the TOE, or malicious operation directed towards the TOE. A potential violation of security.
- **Validation:** The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body:** A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.
- **Vulnerabilities:** A vulnerability is a hardware, firmware, or software flaw that leaves an Automated Information System (AIS) open for potential exploitation. A weakness in automated system security procedures, administrative controls, physical layout, internal controls, and so forth, which could be exploited by a threat to gain unauthorized access to information or disrupt critical processing.

14. BIBLIOGRAPHY

1.) Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated September 2006, Version 3.1, Revision 1, CCMB-2006-09-001.

2.) Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated September 2007, Version 3.1, Revision 2, CCMB-2007-09-002.

3.) Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated September 2007, Version 3.1, Revision 2, CCMB-2007-09-003.

4.) Common Evaluation Methodology for Information Technology Security Evaluation, dated September 2007, Version 3.1, Revision 2, CCMB-2007-09-004.

5.) Avocent Cybex SwitchView SC Series Switches Security Target, Version 6.0, dated April 19, 2011.

6.) Computer Sciences Corporation (CSC): *Evaluation Technical Report for a Target of Evaluation for the Avocent SwitchView SC Series: SC620, SC640, and SC740 Switches, Version 1.0, May 4, 2011*.