National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

Argon Corp Ruggedized KVM Switch Part Number 90731

Report Number: CCEVS-VR-10435-2011

Dated: 20 May 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 Suite 6940
Fort Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

Mario Tinto

The Aerospace Corporation

Columbia, MD

Rick Murphy

Noblis

Falls Church, VA

Common Criteria Testing Laboratory

CSC

7231 Parkway Drive

Hanover, Maryland 21076

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 assessment by the National Information Assurance Partnership (NIAP) validation team of the evaluation of the Argon Corp Ruggedized KVM Switch Part Number 90731, the target of evaluation (TOE), performed by Computer Sciences Corporation the Common Criteria Testing Laboratory (CCTL). It presents the evaluation results, their justifications, and the conformance results. This report is not an endorsement of the TOE by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by Computer Sciences Corporation (CSC) of Hanover, MD in accordance with the United States evaluation scheme and completed on May 5, 2011. The information in this report is largely derived from the ST, the Evaluation Technical Report (ETR) and the functional testing report. The ST was written by Argon Corporation. The evaluation was performed to conform to the requirements of the Common Criteria for Information Technology Security Evaluation, version 3.1, dated September 2006 at Evaluation Assurance Level 4 (EAL 4) augmented with ALC_FLR.2, and the Common Evaluation Methodology for IT Security Evaluation (CEM), Version 3.1, September 2006.

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: DVI-I video, Audio (input and output), USB keyboard, and USB mouse, to be shared among two to four computers. The TOE is a ruggedized peripheral sharing switch (PSS) based on the Avocent SwitchView SC Series SC440 hardware, which was Common Criteria evaluated as VID-10327. This PSS is protected from the elements (e.g. water, wind, debris) by an aluminum case. The switch has a remote set of buttons (connected to the switch by a 12-foot cable) that are large enough to be operated by users who are wearing gloves or other protective equipment. The indicator lights for this TOE are also located on the remote selection device, a custom extension to the Avocent switch, and are plainly visible to users. Due to the inaccessible environment that this PSS is designed to be deployed in, there are no selection buttons or indicator lights on the switch case itself. The PSS is controlled remotely. The Remote Controls under evaluation are: WIRED ASSY, KVM CONTROL PANEL P/N 7432562 manufactured by Lockheed Martin, REMOTE SWITCH CONTROL P/N 100901 manufactured by Argon Corp., and REMOTE SWITCH CONTROL P/N 100429 manufactured by Argon.

The Argon 90731 Switch works with IBM PC compatible and Sun systems and has ports for USB keyboard, USB mouse, DVI-I video and audio (input and output). A CCID Smart Card reader or a CAC reader can be used with the Argon 90731 Switch via a USB interface, but this capability is not included in the evaluated configuration.

The TOE is a peripheral sharing switch. The physical boundary of the TOE consists of one Argon switch and one of three remote controls (see Table 1: TOE Features), and its accompanying User and Administrator Guidance.

Table 1: TOE Features

Model	TOE Identification Part Numbers	Ports	Interfaces
Argon Corp Ruggedized KVM Switch	Switch 90731 and one of the following controls: 7432562, 100901, or 100429	4	USB keyboard, USB mouse, audio (speaker and microphone), DVI-I video monitor interfaces.

In its evaluated configuration, the TOE is connected to a set of human interface devices and one or more computers. The human interface devices and computer(s) are not a part of the TOE. The KVM Switch's security design also ensures that only human interface devices (HIDs) such as keyboards, trackballs, and mice will operate. This prevents unauthorized USB data transfer to or from the connected computers by devices such as USB flash drives, cameras, hard drives and alike. These devices will not function when connected to the Rugged KVM Switch.

The Remote Controls under evaluation are: WIRED ASSY, KVM CONTROL PANEL P/N 7432562 manufactured by Lockheed Martin, REMOTE SWITCH CONTROL P/N 100901 manufactured by Argon Corp., and REMOTE SWITCH CONTROL P/N 100429 manufactured by Argon.

For the TOE to meet an EAL4 assurance level in a Common Criteria evaluated configuration, the selected remote control indicator light must never be dimmed so that it is not visible to the user.

The evaluated TOE configuration excludes the usage of a proprietary USB target selection / indication device if such device becomes available for purchase.

A CCID Smart Card reader or a CAC reader can be used with the Argon 90731 Switch, but this capability is not included in the evaluated configuration.

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 August 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	Argon Corp Ruggedized KVM Switch Part Number 90731
Protection Profile	*Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile, version 1.2*, dated August 21, 2008
Security Target	*Argon Corp Ruggedized KVM Switch Security Target, Document Version .11 May 3, 2011*
Dates of evaluation	August 2010 through April 2011
Evaluation Technical Report	*Argon Corp Ruggedized KVM Switch Part Number 90731, Evaluation Technical Report, Version 2.0, May 5, 2011*
Conformance Result	Part 2 extended and Part 3 EAL 4 augmented with ALC_FLR.2
Common Criteria version	Common Criteria for Information Technology Security Evaluation Version 3.1, September 2006
Common Evaluation Methodology (CEM) version	CEM version 3.1R1, September 2006
Sponsor	Argon Corporation
Developer	Argon Corporation
Evaluators	Gregory Bluher of Computer Sciences Corporation
Validation Team	Mario Tinto , Rick Murphy

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 1.2, dated August 21, 2008.

Signals processed by the TOE are shared peripheral device data, Data Display Channel information, and video signals. 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. Because the TOE uses electrical (hardware) signals, not software logic, to change signal paths for attached computer peripherals, user data is not labeled with the peripheral port group IDs.

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 first computer to be powered on will be the default selected computer until the user selects another. 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 a select LED inside the selected channel button.

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 Operational Security Assumptions

It is assumed that 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]. It is also assumed that only the selected computer's video channel will be visible on the shared monitor. It is assumed that vulnerabilities associated with the 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.

4.4 Threats Countered and Not Countered

The TOE is designed to fully or partially counter the following threats:

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.

4.5 Organizational Security Policies

The *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.2, dated August 21, 2008, 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)
- Security Management (TSF_MGT)

5.1.1 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 1.2, dated August 21, 2008. 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).

5.1.2 Security Management (TSF_MGT)

The TOE allows for the connected computers to be powered-up all-at-once or one at a time. The first computer to be powered on will be the default selected computer until the user selects another. 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 a select LED inside the selected channel button.

5.2 Physical Scope and Boundary

In its evaluated configuration, the TOE is connected to a set of human interface devices and one or more computers. The human interface devices and computer(s) are not a part of the TOE. The KVM Switch's security design also ensures that only human interface devices (HIDs) such as keyboards, trackballs, and mice will operate. This prevents unauthorized USB data transfer to or from the connected computers by devices such as USB flash drives, cameras, hard drives and alike. These devices will not function when connected to the Rugged KVM Switch.

The Remote Controls under evaluation are: WIRED ASSY, KVM CONTROL PANEL P/N 7432562 manufactured by Lockheed Martin, REMOTE SWITCH CONTROL P/N 100901 manufactured by Argon Corp., and REMOTE SWITCH CONTROL P/N 100429 manufactured by Argon.

For the TOE to meet an EAL4 assurance level in a Common Criteria evaluated configuration, the selected remote control indicator light must never be dimmed so that it is not visible to the user. The following figure depicts the TOE and its environment.

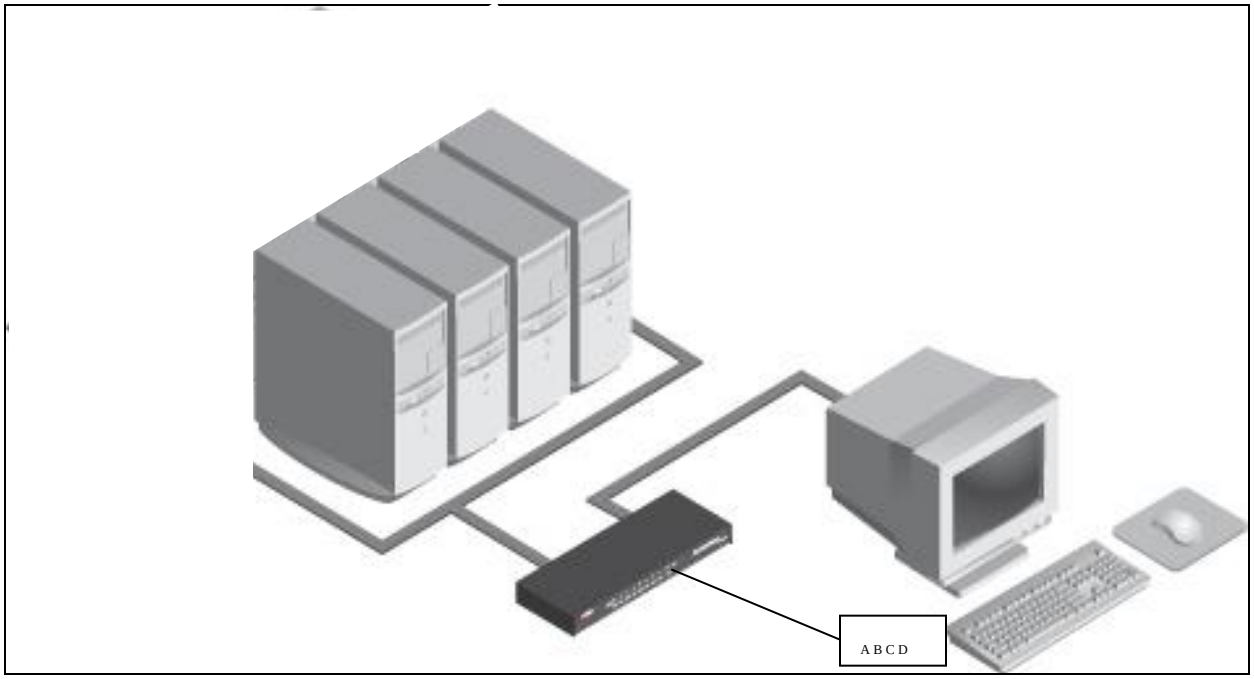


Figure 1: Depiction of TOE Deployment

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 Argon Corp Ruggedized KVM Switch Part Number 90731. Note that not all evidence is available to customers. The following documentation is available to the customer:

- Argon Rugged KVM Switch Operating Manual (90731-702 Rugged KVM Switch Manual Rev. J.pdf)

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.

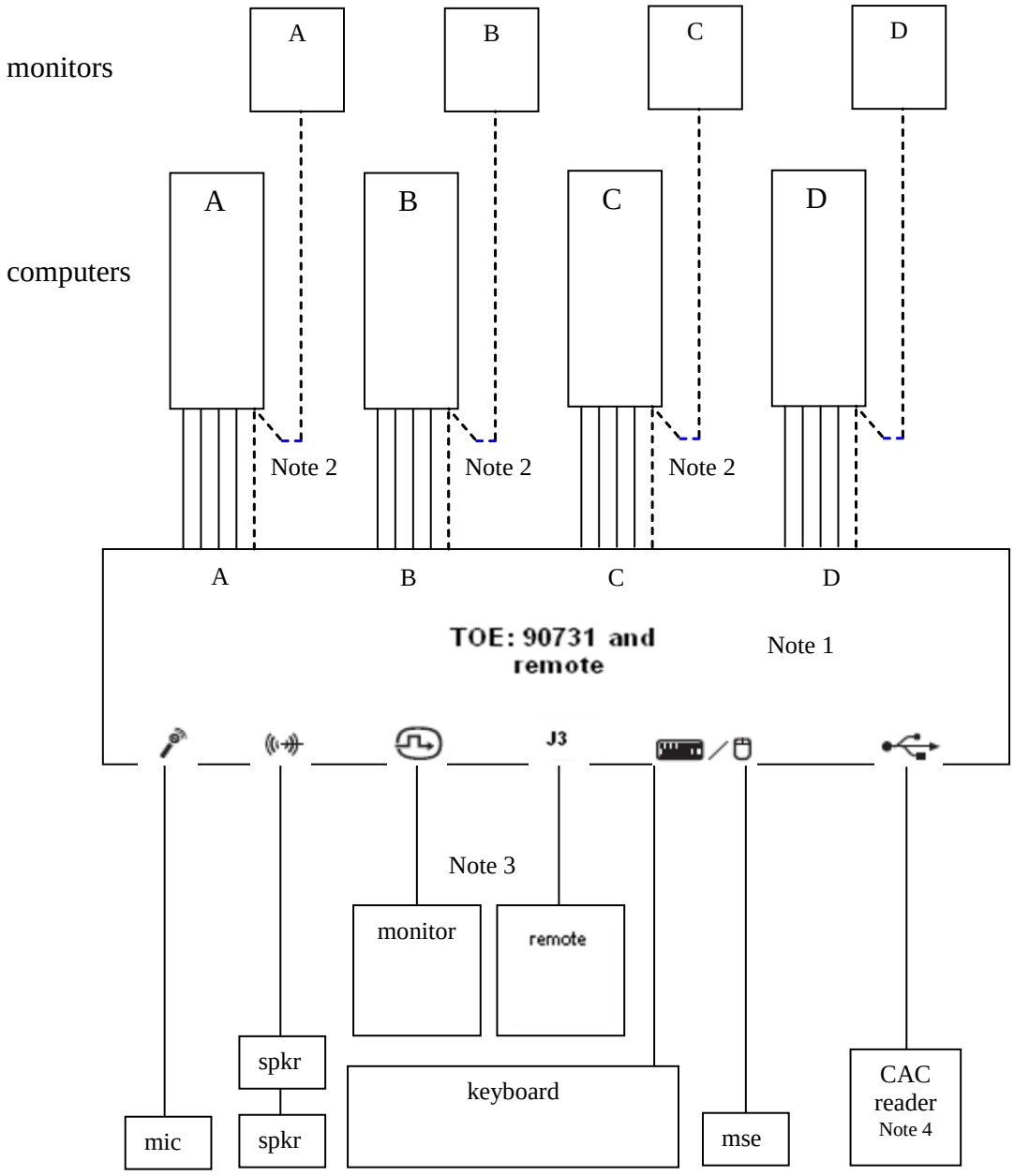
7.1 Developer Testing

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 4. 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 a portion of this test configuration during Independent testing.



Note:

1. Four-button remote set-up is illustrated. Omit computers C and D with two-button remote.

2. Laptop screens serve as Monitors A-D where dictated by test procedure – Smart Card Reader tests, otherwise connect computer video to TOE only and keep the laptops closed.

3. The box to the right of the user monitor labeled “remote” denotes one of the three remotes under evaluation.

4. Smart Card Reader is attached to the TOE via a USB hub it has to share with the keyboard and/or mouse since the TOE has only one USB port capable of handling 2 USB devices.

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, UPS, 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 as well as a subset of the implementation representation and selected 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 for each of the remote controls under evaluation.

7.3 Vulnerability Analysis

The evaluation team gained assurance that the TOE does not contain exploitable flaws or weaknesses in the TOE based 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) 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 of the Argon Corp Ruggedized KVM Switch Part Number 90731, as defined in the Security Target, consists of the switch and one of the three evaluated remotes: WIRED ASSY, KVM CONTROL PANEL P/N 7432562 manufactured by Lockheed Martin, REMOTE SWITCH CONTROL P/N 100901 manufactured by Argon Corp., and REMOTE SWITCH CONTROL P/N 100429 manufactured by Argon.

A CCID Smart Card reader or a CAC reader can be used with the Argon 90731 Switch via a USB interface, but this capability is not included in the evaluated configuration.

The Argon Corp Ruggedized KVM Switch Part Number 90731 must be configured in accordance with the following Guidance Document:

- Argon Rugged KVM Switch Operating Manual (90731-702 Rugged KVM Switch Manual Rev. J.pdf)

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 3.1R1. The evaluation methodology used by the evaluation team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 3.1R1.

Computer Sciences Corporation (CSC) has determined that the product meets the security criteria in the Security Target, which specifies an assurance level of EAL 4 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 April 4, 2011. A final Validation Oversight Review (VOR) was held on April 29, 2011 and final changes to the VR were completed on May 5, 2011.

10. VALIDATOR COMMENTS

It should be noted that Precedent Decision -138 affects the Protection Profile that this TOE conforms with. The customer is urged to review PD-138 (http://www.niap-ccevs.org/cc-scheme/PD/0138.html) as products compliant with this profile may not include mechanisms to ensure that all peripheral memory is cleared when the device is switched between computers. Switching functionality for the Argon Corp Ruggedized KVM Switch includes complete disconnect of the active Host during switching, resulting in the requisite USB reset upon reconnection to the new Host. Through USB enumeration rules, this reset activity eliminates any data stored in a volatile USB buffer within a peripheral device. Any commercially available peripheral (as defined in the referenced Protection Profile) without non volatile memory is assumed to conform to the USB standard.

Although the Argon 90731 Switch supports the use of a CCID Smart Card reader or a CAC reader via the USB interface, it has been determined that this capability is excluded from the evaluated configuration.

It is the responsibility of integrators of the switch to assess the risk of information transfer with compliant devices.

11. ANNEXES

None

12. SECURITY TARGET

Argon Corp Ruggedized KVM Switch Security Target, Document Version .11, May 3, 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.

2.) Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated September 2006, Version 3.1, Revision 1.

3.) Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated September 2006, Version 3.1, Revision 1.

4.) Common Evaluation Methodology for Information Technology Security Evaluation, dated September 2006, Version 3.1, Revision 1.

5.) Argon Corp Ruggedized KVM Switch Security Target, Document Version .10 March 31, 2011.

6.) Computer Sciences Corporation (CSC). *Argon Corp Ruggedized KVM Switch Part Number 90731, Evaluation Technical Report, Version 1.0, April 4, 2011*.