National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

High Security Labs Secure KVM Models SK21D-3, SK21P-3, SK21H-3, SX22D-3, SX22H-3, DK22H-3, DK22P-3, DK22D-3, DK22PD-3, SK41D-3, SK41DU-3, SK41P-3, SK41PU-3, SK41H-3, SK41HU-3, DK42D-3, DK42DU-3, DK42P-3, DK42PU-3, DK42H-3, DK42HU-3, SX42DU-3, SX42PU-3, SX42HU-3, SK81DU-3, DK82DU-3, SK161DU-3

Report Number: CCEVS-VR-VID10983-2019

Dated: 31 July, 2019

Version: 1.5

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

Daniel Faigin

The Aerospace Corporation

John Butterworth

The MITRE Corporation

Common Criteria Testing Laboratory

DXC Technology
10830 Guilford Road, Suite #308
Annapolis Junction, MD 20701

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 High Security Labs Secure KVM Combiner, the Target of Evaluation (TOE), performed by DXC Technology. 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 DXC Technology (DXC) of Hanover MD in accordance with the United States evaluation scheme and completed on July 31, 2019. The information in this report is largely derived from the ST, the Evaluation Technical Report (ETR) and the functional testing report. The evaluation was performed to conform to the requirements of the Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, dated September 2012 at Evaluation Assurance Level 1, and the Common Evaluation Methodology for IT Security Evaluation (CEM), Version 3.1, Revision 4, September 2012 and the NIAP Peripheral Sharing Switch for Human Interface Devices Protection Profile, Version 3.0, February 13, 2015.

The High Sec Labs Secure Peripheral Sharing Switches (PSS) allows the secure sharing of a single set of peripheral components such as keyboard, Video Display and Mouse/Pointing devices among multiple computers through standard USB, DVI, HDMI, and DisplayPort interfaces.

The Evaluation Team performed an analysis of the NIAP Technical Decisions and found that TD0298, published on March 9, 2018, was applicable to this PP. The evaluation team investigated and determined that this technical decision is not applicable to this TOE. The explanation for this, and a list of all Technical Decisions applicable to this PP and TOE, is described in section 3.1 below and in section 2.3 of the Security Target.

The TOE is also compliant with all International interpretations with effective dates on or before May 8, 2019.

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 and NIAP approved Protection Profiles 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 1 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 1: Evaluation Identifiers

Item	**Identifier**
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Target of Evaluation	High Security Labs Secure KVM
Protection Profile	NIAP Peripheral Sharing Switch for Human Interface Devices Protection Profile, Version 3.0, February 13, 2015
Security Target	High Security Labs Secure KVM Security Target, v4.5, July 2019
Dates of evaluation	May 8, 2019 – July 31, 2019
Evaluation Technical Report	HSL KVM Switches Evaluation Technical Report, v.1.2b, July 2019
Assurance Activity Report	HSL KVM Switches Assurance Activity Report, v.1.2, July 2019
Conformance Result	1. Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, CCMB-2012-09-001, Version 3.1 Revision 4, September 2012. 2. Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, CCMB-2012-09-002, Version 3.1 Revision 4, September 2012. 3. Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, CCMB-2012-09-003, Version 3.1 Revision 4, September 2012. 4. Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2012-09-004, Version 3.1, Revision 4, September 2012. The following CC conformance: • Part 2 extended • Part 3 conformant
Common Criteria version	Common Criteria for Information Technology Security Evaluation Version 3.1, Revision 4, September 2012
Common Evaluation Methodology (CEM) version	CEM version 3.1R4, September 2012
Sponsor	High Security Labs
Developer	High Security Labs
Evaluators	Brian Pleffner, Cheryl Dugan
Validation Team	The Aerospace Corporation: Daniel Faigin The MITRE Corporation: John Butterworth

3. SECURITY POLICY

The TOE implements the Data Separation Security Function Policy (SFP) as outlined in Section 4 of the claimed Protection Profile. Isolated USB device emulators are used for the keyboard and mouse. There is one USB device emulator per each connected computer. The use of isolated USB device emulators assures that connected computers will not interact electrically or logically with shared TOE or peripheral resources. Data exchange from computer emulators to device emulators is uses a proprietary protocol called UNIDIR. The UNIDIR protocol is limited to basic HID transactions. No other data may flow between emulators as it is not supported by the limited protocol. Keyboard and mouse data flows are not combined or connected to any other TOE data flow. The keyboard and mouse functions are completely isolated from all other functions (audio, video etc.). There are no shared microcontrollers or any other electronic components. No other external interfaces are coupled to the keyboard and mouse data flow paths.

a. Wireless keyboards are not allowed per applicable user guidance.

b. Wireless mice are not allowed per applicable user guidance.

c. TOE Keyboard and mouse USB console ports are interchangeable.

The video subsystem security policy is described in Section 4 below and in section 7.4 of the ST.

3.1. Technical Decisions

Section 2.3 of the ST and TOE addresses the following technical decisions:

TD0083 - AVA_VAN.1 – Applied.

TD0086 - FDP_IFF.1.5 – Applied.

TD0136 - FDP_RIP.1.1 – Applied.

TD0144 - FDP_RIP.1.1 - Applied.

TD0251 - FMT_MOF.1.1 - Applied.

TD0298 - FDP_IFF.1 Assurance Activities – Not applicable

> **Rationale:** TD0298 changes the testing Assurance Activities for the SFR, but not the SFR. The FDP_IFF.1 requirement is not changed in the ST and is still applicable to the TOE. However, the test steps added by the new TD are not applicable to the TOE under evaluation. These procedures apply to a TOE that supports DisplayPort video format passed through the switch. A TOE that supports DisplayPort through conversion to other video formats through an external cable or dongle should not be tested using these procedures or test steps. All TOE models under evaluation support DisplayPort input by converting DisplayPort to HDMI and therefore are not affected by the TD changes in part 2 of test 4.4. If necessary, the evaluation team is prepared to raise a TRRT to request concurrence or a formal decision based on this rationale.

4. ARCHTECTURAL INFORMATION

The TOE implements the Data Separation Security Function Policy (SFP) as outlined in Section 4 of the claimed Protection Profile.

4.1. Logical Scope and Boundary

Secure KVMs are used to enable a single user having a single set of peripherals to operate in an environment having multiple isolated computers. KVM switches keyboard, mouse, display, audio, and other peripheral devices to one user selected computer.

The following Security Function provides the various KVM TOE features and services that were verified in the current evaluation.

Keyboard and mouse security

The TOE implements isolated keyboard and mouse USB device emulators per connected computer to prevent direct interface between the TOE shared peripheral devices and connected computers.

The TOE uses host (computer) emulators to interface with connected keyboard and mouse peripheral devices, thus isolating external peripherals from TOE internal circuitry and from connected computers.

Keyboard user data is not stored on TOE non-volatile memory. All USB stacks are implemented in the TOE using SRAM (Static Random Access Memory) – a volatile memory that clears data once TOE is powered down.

TOE external interface security

The TOE supports only the following external interfaces protocols:

- USB keyboard and mouse;
- Analog audio output;
- User authentication device or other assigned USB devices (TOE model specific);
- Power (AC or DC); and
- Video (VGA, DVI, HDMI, DisplayPort or MHL video only).

Audio Subsystem security

The TOE audio data flow path is electrically isolated from all other functions and interfaces to prevent signaling data leakages to and from the audio paths.

Video subsystem security

Video input interfaces are isolated from one another. Isolation is achieved through the use of different power and ground planes, different electronic components and different emulated EDID chips per channel.

TOE supports Display Port 1.1, 1.2 and 1.3. TOE video function filters the AUX channel by converting it to I2C EDID only. DisplayPort video is converted into HDMI video stream.

User authentication device subsystem security

TOE supports User Authentication Device function (called DPP or fUSB). These products are configured by default as FDF (Fixed Device Filtration) with filter set to qualify only the following devices:

- Standard smart-card reader USB token or biometric authentication device having USB smart-card class interface complying with USB Organization standard CCID Revision 1.1 or ICCID Revision 1.0.
- Note that device must be bus powered;

User control and monitoring security

TOE is controlled and monitored by the user through front panel illuminated push-buttons and switches. These controls and indications are coupled to the TOE system controller function.

Tampering protection

Always-on anti-tampering system mechanically coupled to the TOE enclosure to detect and attempt to access the TOE internal circuitry.

TOE is equipped with special holographic Tampering Evident Labels that located in critical location on the TOE enclosure.

Self-testing and Log

TOE is equipped with self testing function that operating at TOE power up prior to normal use. The self-test function is running independently at each one of the TOE microcontrollers following power up.

TOE is equipped with event log non-volatile memory that stores information about abnormal security related events.

4.2. Administrative and User configuration of the KVM TOE

The HSL Secure KVM TOE enable user configuration of various minor operational parameters. User may modify these parameters through predefined keyboard shortcuts.

The HSL Secure KVM TOE enable identified and authenticated administrators' configuration of various operational and security parameters. Multiple administrators are supported by the TOE. Access requires user name and password authentication. This access may be performed using one of the following two methods (as further explained in the relevant TOE administrator guidance):

1. Using connected computer and text editor application; and
2. Using special USB configuration loading cable and special configuration utility software.

4.3. Physical Scope and Boundary

The TOE is a peripheral sharing switch configured as a KVM or Mini-Matrix.

The physical boundary of the TOE consists of:

- One HSL Secure KVM Switch or Matrix; Typically (but not necessarily) made internally of system controller board and video board (refer to table 3 below for model and hardware version);
- The firmware embedded inside the TOE that is permanently programmed into the TOE multiple microcontrollers (refer to table 3 below for firmware version);
- The log, state and settings data stored in the TOE;
- The TOE power supply that is shipped with the product (or integrated inside some of the products having 4 ports or more);
- The TOE computer interface cables that are shipped with the product (refer to table 2 below);
- The accompanying User Guidance and Administrator Guidance can be downloaded from High Sec Labs website: http://highseclabs.com/page/?pid=23 at any time.

The evaluated TOE configuration does not include any peripherals or computer components, but does include supplied computer interface cables attached to the TOE. Table 2 below depicts the TOE and Figure 1 below depicts its typical installation environment.

It should be noted that some TOE models support multiple instances of the same peripheral for example Dual Head KVM and Matrix TOE models that support two or more instances of user displays.

It also should be noted that some TOE models support only a partial set of peripheral devices. For example some TOE models do not support user authentication device function (parts are not populated on the board).

4.3.1. Evaluated Environment

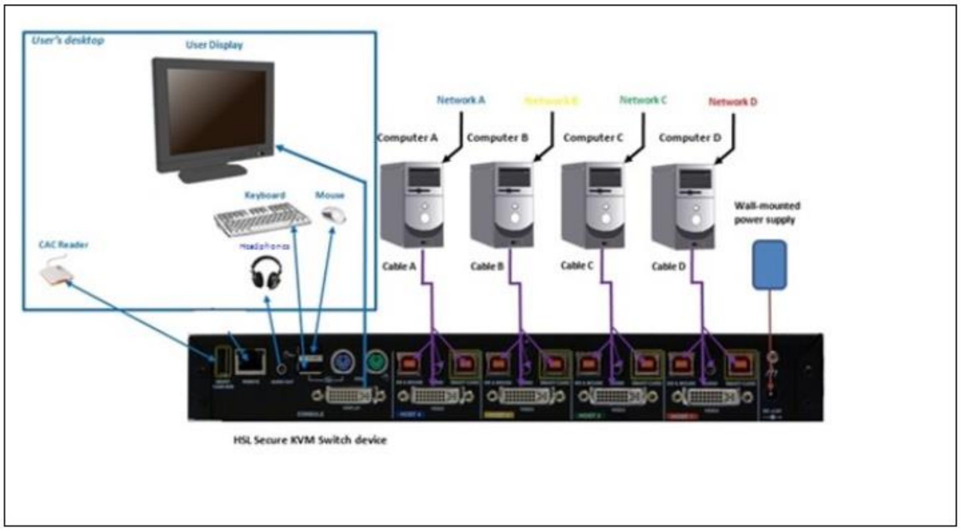
This table identifies hardware components and indicates whether or not each component is in the TOE or Environment.

Table 2: Evaluated TOE and Environment Components

TOE / Environment	Component	Description
TOE	Selectable product from table 2 above.	TOE Hardware and firmware
Environment	Standard USB	Console USB user mouse port
Environment	Standard USB	Console USB user keyboard port

<table>
<tr><td>Environment</td><td>Standard USB User Authentication Device.
Any other predefined USB device based on the Configurable Device Filtration (CDF) settings.</td><td>Console user authentication device interface</td></tr>
<tr><td>TOE</td><td>HSL KVM Cables (as needed):
<table>
<tr><th>P/N</th><th>Description</th></tr>
<tr><td>CWR05117</td><td>KVM Cable short (1.8 m), USB Type-A to USB Type-B, Black</td></tr>
<tr><td>CWR05116</td><td>KVM Cable short (1.8 m), Audio out, DPP, Black</td></tr>
<tr><td>CWR05205</td><td>KVM Cable short (1.8 m), DVI-A to VGA, USB, Black</td></tr>
<tr><td>CWR05114</td><td>KVM Cable short (1.8 m), DVI-D to DVI-D Single-Link, USB, Black</td></tr>
<tr><td>CWR05115</td><td>KVM Cable short (1.8 m), DVI-D to DVI-D Dual-Link, USB, Black</td></tr>
<tr><td>HWR08154</td><td>KVM Cable short (1.8m), HDMI to HDMI, USB, Black</td></tr>
<tr><td>CWR05113</td><td>KVM Cable short (1.8 m), DVI-D to DVI-D Single-Link, USB, Audio out, DPP, Black</td></tr>
<tr><td>CWR06246</td><td>KVM Cable short (1.8 m), DP to DP, USB A to USB B, Black</td></tr>
</table></td><td>Cables for connection of computers to TOE computers</td></tr>
<tr><td>TOE</td><td>Special Administrator Configuration Loading Cable (as needed):
<table>
<tr><th>P/N</th><th>Description</th></tr>
<tr><td>HWR06579</td><td>HSL USB Type-A to USB Type-A Configuration Loading Cable, 1.8m, Black</td></tr>
</table></td><td>USB-A to USB-A Configuration Loading Cable</td></tr>
<tr><td>Environment</td><td>Standard amplified stereo speakers or analog headphones</td><td>Audio output console port</td></tr>
<tr><td>Environment</td><td>Standard PC, Server, portable computer, tablet, thin-client or zero-client running any operating system; or
KVM extender connected to remote platform.</td><td>Connected computers</td></tr>
</table>

Figure 1: Typical example of a KVM TOE installation



4.3.2. KVM TOE details

Table 3: Evaluated KVM Products

Model	P/N	Description	Eval. Version
2-Port			
SK21D-3	CGA10107	HSL Secure SH KVM Switch 2-Port DVI-I video, PP 3.0	33303-C4C4
SK21P-3	CGA10108	HSL Secure SH KVM Switch 2-Port DisplayPort video, PP 3.0	33303-C4C4
SK21H-3	CGA10109	HSL Secure SH KVM Switch 2-Port 4K HDMI video, PP 3.0	33303-C4C4
SX22D-3	CGA10110	HSL Secure SH Mini-Matrix KVM 2-Port x 2 DVI-I video, PP 3.0	33303-C4C4
SX22H-3	CGA10111	HSL Secure SH Mini-Matrix KVM 2-Port x 2 HDMI video, PP 3.0	33303-C4C4
DK22H-3	CGA10113	HSL Secure DH KVM Switch 2-Port 4K HDMI video, PP 3.0	33303-C4C4
DK22P-3	CGA10114	HSL Secure DH KVM Switch 2-Port DisplayPort video, PP 3.0	33303-C4C4
DK22D-3	CGA10115	HSL Secure DH KVM Switch 2-Port DVI-I, PP 3.0	33303-C4C4
DK22PD-3	CGA10116	HSL Secure DH KVM Switch 2-Port DVI-I and DisplayPort, PP 3.0	33303-C4C4
4-Port			
SK41D-3	CGA10129	HSL Secure SH KVM Switch 4-Port DVI-I video, PP 3.0	33303-C4C4
SK41DU-3	CGA10130	HSL Secure SH KVM Switch 4-Port DVI-I video, w/fUSB (2), PP 3.0	33333-C4C4
SK41P-3	CGA10131	HSL Secure SH KVM Switch 4-Port DisplayPort video, PP 3.0	33303-C4C4
SK41PU-3	CGA10132	HSL Secure SH KVM Switch 4-Port DisplayPort video, w/fUSB, PP 3.0	33333-C4C4
SK41H-3	CGA10133	HSL Secure SH KVM Switch 4-Port 4K HDMI video, PP 3.0	33303-C4C4
SK41HU-3	CGA10134	HSL Secure SH KVM Switch 4-Port 4K HDMI video, w/fUSB, PP 3.0	33333-C4C4
DK42D-3	CGA10135	HSL Secure DH KVM Switch 4-Port DVI-I video, PP 3.0	33303-C4C4

DK42DU-3	CGA10136	HSL Secure DH KVM Switch 4-Port DVI-I video, w/fUSB, PP 3.0	33333-C4C4
DK42P-3	CGA10137	HSL Secure DH KVM Switch 4-Port DisplayPort video, PP 3.0	33303-C4C4
DK42PU-3	CGA10138	HSL Secure DH KVM Switch 4-Port DisplayPort video, w/fUSB, PP 3.0	33333-C4C4
DK42H-3	CGA10139	HSL Secure DH KVM Switch 4-Port HDMI video, PP 3.0	33303-C4C4
DK42HU-3	CGA10140	HSL Secure DH KVM Switch 4-Port HDMI video, w/fUSB, PP 3.0	33333-C4C4
SX42DU-3	CGA10143	HSL Secure SH Mini-Matrix KVM 4-Port DVI video, w/fUSB, PP 3.0	33333-C4C4
SX42PU-3	CGA10144	HSL Secure SH Mini-Matrix KVM 4-Port DisplayPort video, w/fUSB, PP 3.0	33333-C4C4
SX42HU-3	CGA10145	HSL Secure SH Mini-Matrix KVM 4-Port HDMI video, w/fUSB, PP 3.0	33333-C4C4
8/16-Port			
SK81DU-3	CGA10149	HSL Secure SH KVM Switch 8-port DVI video w/fUSB, PP 3.0	33333-C4C4
DK82DU-3	CGA10150	HSL Secure DH KVM Switch 8-port DVI video w/fUSB, PP 3.0	33333-C4C4
SK161DU-3	CGA10151	HSL Secure SH KVM Switch 16-port DVI video w/fUSB, PP 3.0	33333-C4C4

5. ASSUMPTIONS AND CLARIFICATION OF SCOPE

5.1. Assumptions

The ST identified the following security assumptions:

Table 4: Secure Usage Assumptions

Assumption	Definition
A.NO_TEMPEST	It is assumed that the computers and peripheral devices connected to the TOE are not TEMPEST approved.
A.NO_SPECIAL_ANALOG_CAPABILITIES	It is assumed that the computers connected to the TOE are not equipped with special analog data collection cards or peripherals such as: Analog to digital interface, high performance audio interface, Digital Signal Processing function, and analog video capture function.
A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
A.TRUSTED_ADMIN	TOE Administrators and users are trusted to follow and apply all guidance in a trusted manner.
A.TRUSTED_CONFIG	Personnel configuring the TOE and its operational environment will follow the applicable security configuration guidance.

5.2. Threats

"Threats to Security" Section 2 of the claimed Protection Profile identifies the following threats to the assets against which specific protection within the TOE is required:

Table 5: Threats

Threat	Definition
T.DATA_LEAK	A connection via the PSS between computers may allow unauthorized data flow through the PSS or its connected peripherals.
T.SIGNAL_LEAK	A connection via the PSS between computers may allow unauthorized data flow through bit-by-bit signaling.
T.RESIDUAL_LEAK	A PSS may leak (partial, residual, or echo) user data between the intended connected computer and another unintended connected computer. More specifically, a PSS may leak user keyboard entries to a PSS-connected computer other than the selected computer in real-time or at a later time.

T.UNINTENDED_SWITCHING	A threat in which the user is connected to a computer other than the one to which they intended to be connected.
T.UNAUTHORIZED_DEVICES	The use of an unauthorized peripheral device with a specific PSS peripheral port may allow unauthorized data flows between connected devices or enable an attack on the PSS or its connected computers.
T.AUTHORIZED_BUT_UNTRUSTED_DEVICES	The use of an authorized peripheral device with the PSS may still cause unauthorized data flows between connected devices or enable an attack on the PSS or its connected computers. Such threats are possible due to known or unknown device vulnerabilities or due to additional functions within the authorized peripheral device.
T.MICROPHONE_USE	Microphone connected to the TOE used for audio eavesdropping or to transfer data across an air-gap through audio signaling.
T.AUDIO_REVERSED	Audio output device used by an attacker as a low-gain microphone for audio eavesdropping. This threat is an abuse of the computer and TOE audio output path to reverse the analog data flow from the headphones to the computer. The computer then amplifies and filters the weak signal, and then digitizes and streams it to another location.
T.LOGICAL_TAMPER	An attached device (computer or peripheral) with malware, or otherwise under the control of a malicious user, could modify or overwrite code embedded in the TOE’s volatile or non-volatile memory to allow unauthorized information flows between connected devices.
T.PHYSICAL_TAMPER	A malicious human agent could physically tamper with or modify the TOE to allow unauthorized information flows between connected devices.
T.REPLACEMENT	A malicious human agent could replace the TOE during shipping, storage, or use with an alternate device that does not enforce the TOE security policies.
T.FAILED	Detectable failure of a PSS may cause an unauthorized information flow, weakening of PSS security functions, or unintended switching.

5.3. Organizational Security Policies

The Protection Profile claimed identifies no Organizational Security Policies (OSPs) to which the TOE must comply.

5.4. Security Objectives for the TOE

The following table, Security Objectives for the TOE, identifies the security objectives of the TOE. These security objectives reflect the stated intent to counter identified threats and/or comply with any security policies identified.

Security Objective	Definition as applied to KVM type TOE
O.COMPUTER_INTERFACE_ISOLATION	The TOE must prevent unauthorized data flow to assure that the TOE and/or its connected peripheral devices would not be exploited in an attempt to leak data. The TOE computer interface shall be isolated from all other TOE computer interfaces while TOE is powered.
O.COMPUTER_INTERFACE_ISOLATION_TOE_UNPOWERED	The same level of isolation defined in the dataflow objectives must be maintained at all times, including periods while TOE is unpowered.
O.USER_DATA_ISOLATION	User data such as keyboard entries should be switched (i.e., routed) by the TOE only to the computer selected by the user. The TOE must provide isolation between the data flowing from the peripheral device to the selected computer and any non-selected computer.
O.NO_USER_DATA_RETENTION	The TOE shall not retain user data after it is powered down.
O.PURGE_TOE_KB_DATA_WHILE_SWITCHING	The TOE shall purge all user keyboard data from computer interfaces following channel switching and before interacting with the new connected computer.
O.NO_DOCKING_PROTOCOLS	The use of docking protocols such as DockPort, USB docking, Thunderbolt etc. is not allowed in the TOE.
O.NO_OTHER_EXTERNAL_INTERFACES	The TOE may not have any wired or wireless external interface with external entities (external entity is an entity outside the TOE evaluated system, its connected computers and peripheral devices).
O.NO_ANALOG_AUDIO_INPUT	Shared audio input peripheral functions (i.e., analog audio microphone input or line input) are not allowed in the TOE.
O.UNIDIRECTIONAL_AUDIO_OUT	The TOE shall be designed to assure that reverse audio signal attenuation will be at least 30 dBv measured with 200 mV and 2V input pure sinus wave at the extended audio frequency range including negative swing signal. The level of the reverse audio signal received by the

	selected computer shall be minimal to assure that the signal level generated by headphones will be well under the noise floor level.
O.COMPUTER_TO_AUDIO_ISOLATION	The audio dataflow shall be isolated from all other TOE functions. Signal attenuation between any TOE computer interface and any TOE audio interface shall be at least 45 dBv measured with 2V input pure sinus wave at the extended audio frequency range including negative swing signal.
O.USER_AUTHENTICATION_ISOLATION	The user authentication function shall be isolated from all other TOE functions.
O.USER_AUTHENTICATION_RESET	Upon switching computers, the TOE shall reset (turn off and then turn on) the power supplied to the user authentication device for at least 1 second
O.USER_AUTHENTICATION_ADMIN	TOE CDF configuration may only performed by an administrator.
O.AUTHORIZED_SWITCHING	The TOE shall allow only authorized switching mechanisms to switch between connected computers and shall explicitly prohibit or ignore unauthorized switching mechanisms.
O.NO_AMBIGUOUS_CONTROL	Only one switching method shall be operative at any given time to prevent ambiguous commands.
O.CONTINUOUS_INDICATION	The TOE shall provide continuous visual indication of the computer to which the user is currently connected.
O.KEYBOARD_AND_MOUSE_TIED	The TOE shall ensure that the keyboard and mouse devices are always switched together
O.NO_CONNECTED_COMPUTER_CONTROL	The TOE shall not allow TOE control through a connected computer.
O.PERIPHERAL_PORTS_ISOLATION	The TOE shall prevent data flow between peripheral devices of different SPFs and the TOE peripheral device ports of different SPFs shall be isolated.
O.DISABLE_UNAUTHORIZED_PERIPHERAL	The TOE shall only allow authorized peripheral device types (See Annex C) per peripheral device port; all other devices shall be identified and then rejected or ignored by the TOE.
O.DISABLE_UNAUTHORIZED_ENDPOINTS	The TOE shall reject unauthorized peripheral devices connected via a USB hub. Alternatively, the TOE may reject all USB hubs.
O.KEYBOARD_MOUSE_EMULATED	The TOE keyboard and pointing device functions shall be emulated (i.e., no electrical connection other than the

	common ground is allowed between peripheral devices and connected computers).
O.KEYBOARD_MOUSE_UNIDIRECTIONAL	The TOE keyboard and pointing device data shall be forced to unidirectional flow from the peripheral device to the switched computer only.
O.UNIDIRECTIONAL_VIDEO	The TOE shall force native video peripheral data (i.e., red, green, blue, and TMDS lines) to unidirectional flow from the switched computer to the connected display device.
O.UNIDIRERCTIONAL_EDID	The TOE shall force the display EDID peripheral data channel to unidirectional flow and only copy once from the display to each one of the appropriate computer interfaces during the TOE power up or reboot sequence. The TOE must prevent any EDID channel write transactions initiated by connected computers.
O.TAMPER_EVIDENT_LABEL	The TOE shall be identifiable as authentic by the user and the user must be made aware of any procedures or other such information to accomplish authentication. This feature must be available upon receipt of the TOE and continue to be available during the TOE deployment. The TOE shall be labeled with at least one visible and one invisible unique identifying tamper-evident marking that can be used to authenticate the device. The TOE manufacturer must maintain complete list of manufactured TOE articles and their respective identification markings' unique identifiers.
O.ANTI_TAMPERING	The TOE shall be physically enclosed so that any attempts to open or otherwise access the internals or modify the connections of the TOE would be evident. This shall be accomplished through the use of an always-on active anti-tampering system that serves to permanently disable the TOE should its enclosure be opened. The TOE shall use an always-on active anti-tampering system to permanently disable the TOE in case physical tampering is detected.
O.ANTI_TAMPERING_BACKUP_POWER	The anti-tampering system must have a backup power source to enable tamper detection while the TOE is unpowered.
O.ANTI_TAMPERING_BACKUP_FAIL_TRIGGER	A failure or depletion of the anti-tampering system backup power source shall trigger TOE to enter tampered state.
O.ANTI_TAMPERING_INDICATION	The TOE shall have clear user indications when tampering is detected.

O.ANTI_TAMPERING_PERMANENTLY_DISABLE_TOE	Once the TOE anti-tampering is triggered, the TOE shall become permanently disabled. No peripheral-to-computer data flows shall be allowed.
O.NO_TOE_ACCESS	The TOE shall be designed so that access to the TOE firmware, software, or its memory via its accessible ports is prevented.
O.SELF_TEST	The TOE shall perform self-tests following power up or powered reset.
O.SELF_TEST_FAIL_TOE_DISABLE	Upon critical failure detection the TOE shall disable normal operation of the whole TOE or the respective failed component.
O.SELF_TEST_FAIL_INDICATION	The TOE shall provide clear and visible user indications in the case of a self-test failure.

Notes:

1. Objective O.USER_AUTHENTICATION_TERMINATION is not applicable to the Secure KVM and Matrix TOE per referenced PP as it does not support an emulated user authentication device function.
2. O.DISPLAYPORT_AUX_FILTERING is not applicable for HSL KVM TOEs as none of the TOE support DisplayPort display (Native DisplayPort format video).

5.5. Security Objectives for the IT Environment

The following IT security objectives for the environment are to be addressed by the Operational Environment by technical means.

Environment Security Objective	Definition
OE. NO_TEMPEST	The operational environment will not require the use of TEMPEST approved equipment.
OE. NO_SPECIAL_ANALOG_CAPABILITIES	The operational environment will not require special analog data collection cards or peripherals such as: Analog to digital interface, high performance audio interface, Digital Signal Processing function, and analog video capture function.
OE.PHYSICAL	The operational environment will provide physical security, commensurate with the value of the TOE and the data it contains.
OE.TRUSTED_ADMIN	The operational environment will ensure that appropriately trained and trusted TOE Administrators

	and users are available to administer, configure and use the TOE.

5.6. Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance. The level of assurance for this evaluation is defined within the Protection Profile for Peripheral Sharing Switches.

Consistent with the expectations of the Protection Profile, this evaluation did not specifically search for, nor seriously attempt to counter, vulnerabilities that were not “obvious” or vulnerabilities to objectives not claimed in the ST. The CEM defines an “obvious” vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.

The evaluation of security functionality of the product was limited to the functionality specified in the claimed PPs. Any additional security related functional capabilities included in the product were not covered by this evaluation.

The evaluated configuration of the TOE includes the products identified in Table 3 above and in Section 1.3.2 in the ST using the identified version in the same section for each product. The TOE includes all the code that enforces the policies identified.

6. DOCUMENTATION

The following guidance documents are provided with the TOE upon delivery in accordance with the PP:

1. SECURE KVM SWITCH 2 PORT DH USER MANUAL, Rev E
2. SECURE KVM SWITCH 8-16 PORT USER MANUAL, Rev E
3. SECURE KVM SWITCH 2 PORT SH USER MANUAL, Rev E
4. SECURE KVM SWITCH 4 PORT SH USER MANUAL, Rev E
5. 4-PORT SECURE KVM MINI-MATRIX USER MANUAL, Rev E
6. 2-PORT SECURE KVM MINI-MATRIX USER MANUAL, Rev E
7. SECURE KVM SWITCH 4 PORT DH USER MANUAL, Rev E
8. HSL DK22PD-MIXED DUAL KVM USER MANUAL, Rev E
9. HSL fUSB Configuration Manual, Rev C
10. HSL Administrator Guide, Rev E

All documentation delivered with the product is relevant to and within the scope of the TOE.

The accompanying User Guidance and Administrator Guidance can be downloaded from High Sec Labs website: http://highseclabs.com/page/?pid=23 at any time.

7. IT PRODUCT TESTING

This section describes the testing efforts of the evaluation team.

7.1. Evaluation team independent testing

The evaluation team conducted independent testing at the HSL facilities in Huntsville, Alabama. 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. 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 Protection Profile test procedures as a basis for creating each of the Independent tests as required by the Assurance Activities.

Each Assurance Activity was tested as required by the conformant Protection Profiles and the evaluation team verified that each test passed.

7.2. Vulnerability analysis

The evaluation team performed a vulnerability analysis of the TOE evidence and a search of publicly available information to identify potential vulnerabilities in the TOE. Based on the results of this effort, there were no identifiable vulnerabilities found at the time of certification.

8. 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 3.1R4. The evaluation methodology used by the evaluation team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 3.1R4.

DXC Technology (DXC) has determined that the product meets the security criteria in the Security Target, which specifies conformance to the NIAP Peripheral Sharing Switch for Human Interface Devices Protection Profile, Version 3.0, February 13, 2015. A team of Validators, on behalf of the CCEVS Validation Body, monitored the evaluation. The evaluation effort was finished on July 31, 2019.

9. VALIDATOR COMMENTS

The validation team's observations support the evaluation team's conclusion that the High Security Labs Secure KVM meets the claims stated in the Security Target.

The validators suggest that the consumer pay particular attention to the evaluated configuration of the device(s). The functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target, and only the functionality implemented by the SFR's within the Security Target was evaluated. All other functionality provided by the devices, to include software that was not part of the evaluated configuration, needs to be assessed separately and no further conclusions can be drawn about their effectiveness.

Consumers employing the devices must follow the configuration instructions provided in the Configuration Guidance documentation listed in Section 6 to ensure the evaluated configuration is established and maintained.

9.1. Validation Approach

This product was a reevaluation of a product originally evaluated as VID 10701 which had previously underwent assurance maintenance on March 19, 2018 with no changes to the evaluated product. As there were no changes in the implementation of the product, model, or version number, the goal was to reuse as much previous evidence as possible; additional testing of an unchanged product would be superfluous.

The approach taken by the validation team was to:

1. Ensure that all TDs had been addressed in the evaluation and that any impact on assurance activities was assessed and addressed.
2. Evaluate the equivalence arguments to ensure there were no changes to the product that would impact testing, require re-testing, or would be categorized as something other than minor under assurance maintenance.
3. Compare the updated evaluation documentation to the prior evaluation documentation to understand any changes and their rationale, and to ensure any changes remained technically correct.
4. Ensure that the evaluation team reviewed all prior evaluation material to ensure that it remained applicable to the updated evaluation.

10. ANNEXES

None

11. SECURITY TARGET

High Security Labs Secure KVM Security Target, Revision 4.5, July 2019.

12. GLOSSARY

- **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.

13. BIBLIOGRAPHY

1. Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, CCMB-2012-09-001, Version 3.1 Revision 4, September 2012.
2. Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, CCMB-2012-09-002, Version 3.1 Revision 4, September 2012.
3. Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, CCMB-2012-09-003, Version 3.1 Revision 4, September 2012.
4. Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2012-09-004, Version 3.1, Revision 4, September 2012.
5. High Security Labs Secure KVM Security Target, Revision 4.5, July 2019.
6. DXC Technology (DXC): High Security Labs Secure KVM Assurance Activity Report, 1.2, July 2019.