Assurance Activities Report

for

BAE Systems Secure KVM Gen2 8560943-2

Version 1.1

January 10, 2023

Prepared by:

Leidos Inc.
https://www.leidos.com/CC-FIPS140
Common Criteria Testing Laboratory
6841 Benjamin Franklin Drive
Columbia, MD 21046

Prepared for:

National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

The Developer of the TOE:

BAE Systems
450 Pulsaki Road
Greenlawn, NY 11740

The TOE Evaluation was Sponsored by:

BAE Systems
450 Pulsaki Road
Greenlawn, NY 11740

Evaluation Personnel:

Justin Fisher
Josh Marciante
Armin Najafabadi
Allen Sant

Contents

1 Introduction

This document presents results from performing Evaluation Activities (EAs) associated with the evaluation of the BAE Systems Secure KVM Gen2 (8560943-2) peripheral sharing device. This report contains sections documenting the performance of EAs associated with each of the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) as specified in EAs for the individual components of the PP-Configuration for Peripheral Sharing Device, Keyboard/Mouse Devices, and Video/Display Devices, including the following optional and selection-based SFRs:

Protection Profile for Peripheral Sharing Device [PSD PP]:

- FDP_SWI_EXT.2
- FTA_CIN_EXT.1

PP-Module for Keyboard/Mouse Devices [KM Module]:

- FDP_FIL_EXT.1/KM
- FDP_RIP.1/KM
- FDP_SWI_EXT.3

PP-Module for Video/Display Devices [VI Module]:

- FDP_CDS_EXT.1
- FDP_IPC_EXT.1
- FDP_SPR_EXT.1/DP

1.1 Applicable Technical Decisions

The NIAP Technical Decisions referenced below apply to [PSD PP] and the claimed PP-Modules. Rationale is included for those Technical Decisions that do not apply to this evaluation.

TD0506: Missing Steps to disconnect and reconnect display

This TD is applicable to the TOE.

TD0507: Clarification on USB plug type

This TD is applicable to the TOE.

TD0514: Correction to MOD_VI FDP_APC_EXT.1 Test 3 Step 6

This TD is applicable to the TOE.

TD0518: Typographical error in Dependency Table

This TD is applicable to the TOE, but the TD affects the content of the claimed PP and does not affect the claimed SFRs or how they are evaluated.

TD0539: Incorrect selection trigger in FTA_CIN_EXT.1 in MOD_VI_V1.0

The TD is not applicable to the TOE; the TOE does not fit the combiner use case.

TD0583: FPT_PHP.3 modified for PSD remote controllers

This TD is not applicable to the TOE because FPT_PHP.3 is not claimed.

TD0584: Update to FDP APC_EXT.1 Video Tests

This TD is applicable to the TOE

TD0586: DisplayPort and HDMI Interfaces in FDP_IPC_EXT.1

This TD is applicable to the TOE.

TD0593: Equivalency Arguments for PSD

This TD is applicable to the TOE.

TD0620: EDID Read Requirements

This TD is applicable to the TOE.

TD0686: DisplayPort CEC Testing

This TD is applicable to the TOE.

1.2 Evidence

[PSD PP]	Protection Profile for Peripheral Sharing Device, Version 4.0, July 19, 2019
[KM Module]	PP-Module for Keyboard/Mouse Devices, Version 1.0, July 19, 2019
[KM-SD]	Supporting Document for PP-Module for Keyboard/Mouse Devices, Version 1.0, July 19, 2019
[VI Module]	PP-Module for Video/Display Devices, Version 1.0, July 19, 2019
[VI-SD]	Supporting Document for PP-Module for Keyboard/Mouse Devices, Version 1.0, July 19, 2019
[User]	BAE Systems Generation 2 Keyboard, Video, Mouse Switch (KVM) User's Guide (P/N: 8560943-2), January 10, 2023
[Isolation]	BAE Systems Secure KVM Gen2 8560943-2 Isolation Documentation and Assessment, Version 1.0, November 2, 2022 (BAE Systems Proprietary)
[Test]	BAE Systems Secure KVM PSD PP 4.0 Common Criteria Common Criteria Test Report and Procedures, Version 1.1, January 10, 2023
[ST]	BAE Systems Secure KVM Gen2 8560943-2 Security Target, Version 1.0, January 10, 2023
[VA]	BAE Systems Secure KVM Gen2 8560943-2 Vulnerability Survey, Version 1.1, January 10, 2023

1.3 Conformance Claims

Common Criteria Versions

- Common Criteria for Information Technology Security Evaluation Part 1: Introduction, Version 3.1, Revision 5, dated: April 2017.
- Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Components, Revision 5, dated: April 2017.

- Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Components, Revision 5, dated: April 2017.

Common Evaluation Methodology Versions

- Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 5, dated: April 2017.

Protection Profiles

- [PSD PP] Protection Profile for Peripheral Sharing Device, Version 4.0, July 19, 2019
- [KM Module] PP-Module for Keyboard/Mouse Devices, Version 1.0, July 19, 2019
- [VI Module] PP-Module for Video/Display Devices, Version 1.0, July 19, 2019

1.4 SAR Evaluation

The following Security Assurance Requirements (SARs) were evaluated during the evaluation of the TOE:

SAR	Verdict
ASE_CCL.1	Pass
ASE_ECD.1	Pass
ASE_INT.1	Pass
ASE_OBJ.2	Pass
ASE_REQ.2	Pass
ASE_TSS.1	Pass
ADV_FSP.1	Pass
AGD_OPE.1	Pass
AGD_PRE.1	Pass
ALC_CMC.1	Pass
ALC_CMS.1	Pass
ATE_IND.1	Pass
AVA_VAN.1	Pass

The evaluation work units are listed in the proprietary ETR. The evaluators note per the PP evaluation activities that many of the SARs were successfully evaluated through completion of the associated evaluation activities present in the claimed PP and PP-Modules.

2 Security Functional Requirement Evaluation Activities (PSD PP)

This section describes the evaluation activities associated with the SFRs defined in the ST and the results of those activities as performed by the evaluation team. The evaluation activities are derived from [PSD PP] and associated PP-Modules, modified by applicable NIAP Technical Decisions. Evaluation activities for SFRs not claimed by the TOE have been omitted.

Evaluator notes, such as changes made as a result of NIAP Technical Decisions, are highlighted in **bold text**, as are changes made as a result of NIAP Technical Decisions. Bold text is also used within evaluation activities to identify when they are mapped to individual SFR elements rather than the component level.

When the evaluator references a random port; the port is chosen at random for that individual test in such a manner that the vendor supplying the device cannot predict which port will be selected. However, due to the nature of picking a random port there may be cases where the same port is chosen for multiple individual tests this case will be attempted to be avoided though will not exclusively be avoided.

2.1 Mandatory SFRs

2.1.1 User Data Protection (FDP)

2.1.1.1 FDP_APC_EXT.1 Active PSD Connections

2.1.1.1.1 TSS Evaluation Activities

The evaluator shall verify that the TSS describes the conditions under which the TOE enters a failure state.

Section 6.2.1 of [ST] states that the TOE enters a temporary failure state if there is a self-test failure and that this happens if the power-on or run-time self tests fail. Section 6.2.4 of [ST] enumerates the various self-tests that are performed, what condition will cause the self-test to fail, and what the specific failure state is that the TOE enters in response to the failure.

PSD:KM
There are no TSS EAs for this component beyond what the PSD PP requires.

N/A

PSD:VI
There are no TSS EAs for this component beyond what the PSD PP requires.

N/A

2.1.1.1.2 Guidance Activities

The evaluator shall verify that the operational user guidance describes how a user knows when the TOE enters a failure state.

[User] section 4 lists the self-tests that are performed and how those self-test failures are communicated to the user. Specifically:

- The KVM Rx Fault LED, if illuminated, indicates a failure of the KVM receiver module or a failure of logical communications with a transmitter once established. There is a single KVM Rx Fault LED.

- Section 2 of [User] also notes that the KVM Rx Fault LED is illuminated during initial start-up of the TOE and will turn off once start-up is successful.

- The KVM Tx Fault LEDs, if illuminated, indicate a failure of a KVM transmitter module or a failure to establish logical communications with a transmitter (e.g. because the transmitter is disconnected). There is one KVM Tx Fault LED for each transmitter.
- The Invalid KVM VID/PID LED, if illuminated, indicates that an unauthorized peripheral device was connected to a TOE USB peripheral port.
- The Keyboard Fault LED, if illuminated, indicates a failure of the keyboard or the embedded channel selection keys in the wired remote control (e.g. a stuck button).
- The Console Power Supply tests AC voltage, DC voltage, AC input phase, and temperature. In the event of an AC input phase or temperature failure, the self-test failure is indicated through immediate power-down of the TOE. In the event of a voltage failure, the AC OK (AC) or BIT (DC) light on the power supply turns red and a fault light is illuminated on the Power Control Panel.

PSD:KM
There are no guidance EAs for this component beyond what the PSD PP requires.

N/A

PSD:VI
There are no guidance EAs for this component beyond what the PSD PP requires.

N/A

2.1.1.1.3 Test Activities

There are no test Evaluation Activities for this component.

N/A

PSD:KM
For tests that use the USB sniffer or USB analyzer software, the evaluator verifies whether traffic is sent or not sent by inspection of the passing USB transactions and ensuring they do not contain USB data payloads other than any expected traffic, as well as USB NAK transactions or system messages. To avoid clutter during USB traffic capture, the evaluator may filter NAK transactions and system messages.
The evaluator shall perform the following tests.

PSD:KM
Test 1-KM – KM Switching methods
[Conditional: Perform this test if "switching can be initiated only through express user action" is selected in FDP_SWI_EXT.1.1 in the PSD PP]
While performing this test, ensure that switching is always initiated through express user action.
This test verifies the functionality of the TOE's KM switching methods.
Step 1: Configure the TOE and the Operational Environment in accordance with the operational guidance. Connect an authorized peripheral device for each peripheral device type selected in FDP_PDC_EXT.3.1/KM. Run an instance of a text editor on each connected computer.

Step 2: Connect a display to each computer in order to see all computers at the same time, turn on the TOE, and enter text or move the cursor to verify which connected computer is selected.

Step 3: For each switching method selected in FDP_SWI_EXT.2.2, switch selected computers in accordance with the operational user guidance, and verify that it succeeds.

Step 4: For each peripheral device type selected in FDP_PDC_EXT.3.1/KM, attempt to switch the device to more than one computer at once and verify that the TOE ignores all such commands or otherwise prevents the operation from executing.

Step 5: [Conditional: If "keyboard" is selected in FDP_PDC_EXT.3.1/KM, then] attempt to control the computer selection using the following standard keyboard shortcuts, where '#' represents a computer channel number, and verify that the selected computer is not switched:

- Control - Control - # - Enter
- Shift - Shift - #
- Num Lock - Minus - #
- Scroll Lock - Scroll Lock - #
- Scroll Lock - Scroll Lock - Function #
- Scroll Lock - Scroll Lock - arrow (up or down)
- Scroll Lock - Scroll Lock - # - enter
- Control - Shift - Alt - # - Enter
- Alt - Control - Shift - #

Step 6: [Conditional: If "mouse" is selected in FDP_PDC_EXT.3.1/KM, then] attempt to switch to other connected computers using the pointing device and verify that it does not succeed.

Step 7: [Conditional: If "peripheral devices using a guard" is selected in FDP_SWI_EXT.2.2, then] attempt to switch to other connected computers using the peripheral device and guard by only performing some of the steps outlined in the operational user guidance, and verify that it does not succeed.

For this test, the evaluator verified that the three test computers were connected to the TOE's three transmitter ports in the correct order, per the operational guidance. The keyboard, trackball, and touch panel peripherals were connected to the receiver. The evaluator also ensured that the two flat panel displays bundled with the environmental console were connected to the receiver.

The test computers were powered on, as was the TOE.

The evaluator engaged the manual switching mechanism specified in FDP_SWI_EXT.2.2. For each channel, the evaluator observed that the corresponding computer was activated when the channel selection occurred, and that peripheral actions were recorded on the intended computer. There is only one switching mechanism used by the TOE.

The evaluator attempted to switch to more than one computer at once through various methods of attempting to push multiple selection keys (simultaneously, sequentially) and observed that in all cases, the TOE switches to the first computer chosen after the function key is pressed to engage the channel selection.

The evaluator attempted to control the behavior of the switching mechanism by using the various keyboard shortcuts listed in the evaluation activity, with the exception of those involving Num Lock, as the environmental keyboard physically does not have a Num Lock key (in subsequent testing the evaluators observed the proper behavior of fixed device filtration to show that a substitute keyboard is not accepted).

The evaluator used both the trackball and touch panel and verified that these can only be used to control the behavior of the selected computer (e.g., scrolling or swiping does not command the KVM to perform a switching operation).

"Peripheral devices using a guard" is not selected in FDP_SWI_EXT.2.2.

PSD:KM

Test 2-KM – Positive and Negative Keyboard and Mouse Data Flow Rules Testing

This test verifies the functionality for correct data flows of a mouse and keyboard during different power states of the selected computer.

Step 1: Continue with the test setup from Test 1 and for each connected computer, connect a USB sniffer between it and the TOE or open the USB analyzer software. Perform steps 2-12 with each connected computer as the selected computer.

Step 2: Exercise the functions of the peripheral device type selected in FDP_PDC_EXT.3.1/KM and verify that the expected results are observed on the selected computer and that the expected traffic is sent and captured using the USB analyzer.

[Conditional: Perform steps 3-10 if "switching can be initiated only through express user action" is selected in FDP_SWI_EXT.1.1 in the PSD PP.]

Step 3: [If "mouse" is selected in FDP_PDC_EXT.3.1/KM, then] switch the TOE to each connected computer, and use the mouse to position the mouse cursor at the center of each display. Switch the TOE back to the originally selected computer.

Step 4: [If "keyboard is selected in FDP_PDC_EXT.3.1/KM, then] use the keyboard to enter text into the text editor. [If "mouse" is selected in FDP_PDC_EXT.3.1/KM, then] use the mouse to move the cursor to the bottom right corner of the display.

Step 5: Switch to each connected computer and verify that the actions taken in Step 4 did not occur on any of the non-selected computers.

Step 6: Switch to the originally selected computer. Continue exercising the functions of the peripheral device(s) and examine the USB protocol analyzers on each one of the non-selected computers and verify that no traffic is sent.

Step 7: Disconnect and reconnect the TOE interface cables connected to the selected computer. Examine the USB protocol analyzers on each one of the non-selected computers and verify that no traffic is sent.

Step 8: Reboot the selected computer. Examine the USB protocol analyzers on each one of the non-selected computers and verify that no traffic is sent.

Step 9: Enter sleep or suspend mode in the selected computer. Examine the USB protocol analyzers on each one of the non-selected computers to verify that no traffic is sent.

Step 10: Exit sleep or suspend mode on the selected computer. Examine the USB protocol analyzers on each of the non-selected computers to verify that no traffic is sent. Ensure that any text in the Text Editor application is deleted.

Step 11: Perform step 12 when the TOE is off and then in a failure state.

Step 12: Exercise the functions of the peripheral device type selected in FDP_PDC_EXT.3.1/KM and verify that no results are observed on the selected computer and that no traffic is captured using the USB analyzer.

For each connected computer, the evaluator connected a USB sniffer between the connected computer and the TOE. The evaluator observed that keyboard, trackball, and touch panel actions are recorded on the screen and captured by the USB analyzer software.

For each connected computer, the evaluator switched the TOE to that computer, opened a text editor, and put the mouse cursor in a known location. The evaluator switched to each computer, performed keyboard/mouse actions on that computer, then switched to the other computers and verified the same actions were not taken on them.

The evaluator verified, for each computer when selected, that the following behavior on the selected computer did not result in USB traffic being detected on the other computers:

- Using the connected peripherals
- Disconnecting the computer peripheral cables from the TOE

- Rebooting the computer
- Putting the computer into a suspended state
- Taking the computer out of the suspended state

The evaluator powered down the TOE and observed that peripheral actions were not observed on the transmitter side of the TOE (i.e. the signals did not transit the TOE while it was unpowered).

The evaluator placed the TOE into a failure state by inducing a receiver fault error and observed that peripheral data does not transit the TOE.

PSD:KM

Test 3-KM – Flow Isolation and Unidirectional Rule

This test verifies that the TOE properly enforces unidirectional flow and isolation.

Step 1: Ensure the TOE and the Operational Environment are configured in accordance with the operational guidance.

Perform steps 2-12 with each connected computer as the selected computer.

Step 2: Ensure the TOE is powered on and connect a display directly to the selected computer. Open a real-time hardware information console on the selected computer.

[If "mouse" is selected in FDP_PDC_EXT.3.1/KM, then perform steps 3-4]

Step 3: Connect a gaming mouse with programmable LEDs directly to the selected computer and attempt to configure the LEDs using the mouse application running on the selected computer. Verify that the mouse programmable LEDs change state.

Step 4: Disconnect the gaming mouse from the selected computer and connect it to the TOE mouse peripheral device port through the USB sniffer. Attempt to configure the LEDs using the mouse application running on the selected computer. Verify that the mouse programmable LEDs do not change state and that no traffic is sent and captured by the USB sniffer while the evaluator is not moving the mouse.

[If "keyboard" is selected in FDP_PDC_EXT.3.1/KM, then perform step 5]

Step 5: Connect a keyboard to the peripheral device interface through the USB sniffer. Use a keyboard emulation software application running on the selected computer to turn the keyboard Num Lock, Caps Lock, and Scroll Lock LEDs on and off. Verify that the LEDs on the keyboard do not change state and that no traffic is sent and captured by the USB sniffer.

Step 6: Power down the TOE and disconnect the peripheral interface USB cable from the TOE to the selected computer and the peripheral devices from the TOE.

Step 7: Power up the TOE and ensure the selected computer has not changed (this should have no effect on the selected computer because it was disconnected in the previous step). Reconnect the peripheral devices disconnected in step 6 to the TOE.

Step 8: [If "mouse" is selected in FDP_PDC_EXT.3.1/KM, then] check that immediately following the connection, the mouse LEDs are illuminated (indicating that the peripheral devices are powered on, although the selected computer is not connected). [If "keyboard" is selected in FDP_PDC_EXT.3.1/KM, then] check that immediately following the connection, the Num Lock, Caps Lock, and Scroll Lock keyboard LEDs are blinking momentarily and then stay off (indicating that the keyboard is powered on, although the selected computer is not connected).

Step 9: Turn the TOE off and disconnect the peripheral devices connected in step 6.

Step 10: Reconnect the first computer interface USB cable to the TOE.

Step 11: Turn on the TOE and check the computer real-time hardware information console for the presence of the peripheral devices connected in step 6 and disconnected in step 9. The presence of the TOE peripheral devices in the information console when the peripheral devices are not connected to the TOE indicates that the TOE emulates the KM devices.

Step 12: [Conditional] If the TOE keyboard and mouse do not appear in the listed devices, repeat the following steps for both mouse and keyboard to simulate USB traffic:

- Connect a USB generator to the TOE peripheral device interface port.

- Configure the USB generator to enumerate as a generic HID mouse/keyboard device and then to generate a random stream of mouse/keyboard report packets.
- Connect a USB sniffer device between the TOE computer interface and the USB port on the first computer to capture the USB traffic between the TOE and the first computer.
- Turn on the TOE and verify that no packets cross the TOE following the device enumeration.

Note that the normal behavior of the TOE is to explicitly place the keyboard, trackball, and HID input for the touch panel display on an allowlist, such that only the peripheral devices shipped with the TOE as part of the overall workstation are allowed to connect to it. In order to test unidirectionality of the HID data flow, the vendor devised a special firmware build that would allow for the connection of a specific gaming mouse by placing it on the allowlist.

The evaluator connected a gaming mouse directly to one of the computers and verified that the computer recognized the gaming mouse and allowed for configuration of the gaming mouse. The evaluator connected the mouse through the TOE and verified that the computer no longer recognized the gaming mouse and did not permit configuration of the mouse.

The evaluator demonstrated the unidirectionality of the keyboard data flow by showing that data flowed from the peripheral to the connected computer through entry of keyboard commands and toggling of caps and scroll lock indicators and that data did not flow back to the keyboard HID interface from the connected computer. This was done through the following:

- Disconnecting the RS-232 interface from the keyboard to the Rx while the USB connection remained intact and observing that keyboard inputs continued to function but that the caps/scroll lock status indicators did not change.
- Disconnecting the USB interface from the keyboard to the Rx while the RS-232 connection remained intact and observing that keyboard inputs did not function but that the caps/scroll lock status indicators changed in response to changes initiated from the on screen keyboard

The evaluator verified that the TOE emulated the keyboard and mouse devices to all connected computers all the time this was verified through disconnecting the trackball and keyboard from the TOE and observing that the TOE still sent the emulated HID devices to the connected computer. Step 12 was not applicable to the TOE because it is only performed if keyboard/mouse devices are not emulated.

PSD:KM

[TD0507]: Clarification on USB plug type

Test 4-KM – No Flow between Computer Interfaces

[Conditional: Perform this test if “switching can be initiated only through express user action” is selected in FDP_SWI_EXT.1.1 in the PSD PP]

This test verifies correct data flow while the TOE is powered on or powered off.

Step 1: Ensure the TOE and the Operational Environment are configured in accordance with the operational guidance. Connect a display directly to each connected computer. Perform steps 2-10 for each connected computer.

Step 2: Connect a USB sniffer between a non-selected TOE KM computer interface and its computer. Run USB protocol analyzer software on all remaining computers.

Step 3: Turn on the TOE and observe the TOE enumeration data flow in the protocol analyzer connected to the selected computer and is not in any other USB protocol analyzers or the USB sniffer.

Step 4: Ensure the TOE is switched to the first computer.

Step 5: Reboot the first computer. Verify that no USB traffic is captured on all non-selected computer USB protocol analyzers.

Step 6: Generate intensive USB HID traffic by moving the mouse at high speed and/or holding down the keyboard space key at the same time. Verify that no new USB traffic is captured on all non-selected computer USB protocol analyzers.

Step 7: Perform steps 8 and 9 for each TOE keyboard/mouse peripheral interface.

Step 8: Connect a USB dummy load into the TOE KM peripheral device interface. Verify that no new USB traffic is captured on all non-selected computer USB protocol analyzers. Remove the plug after the step is completed.

Step 9: Connect a switchable 5 volt power supply with *any compatible USB plug* into the TOE KM peripheral device interface. Modulate the 5 volt supply (i.e., cycle on and off) manually at various speeds from approximately one cycle per five seconds to one cycle per second. Verify that no new USB traffic is captured on all non-selected computer USB analyzers.

Step 10: Turn off the TOE. Verify that no new traffic is captured.

For this test, each port was selected in turn and for each selected port, both non-selected ports were observed. This was done by using two computers: one computer was connected to the selected port, and a second computer was connected to a non-selected port through a USB sniffer. Once the behavior of the non-selected port was observed, the evaluator moved the second computer to a different non-selected port and repeated the test. This was done until all non-selected ports were observed, after which the first computer was moved to a different active port as the selected port and the process was repeated.

The evaluator verified that when the TOE is rebooted and intensive USB HID traffic is generated, the only communication to each of the other connected computers is the device enumeration communication from the TOE that emulates the connection to each of the connected computers. Validation that HID traffic does not traverse to non-selected ports is covered by FDP_APC_EXT.1 Test 2-KM, Step 6.

The evaluator connected a dummy USB device and verified that no new data packets are transferred across to other computers. The evaluator connected 5 V power unit capable of modulation to the TOE via USB Type-A and verified that no data is transferred to the other computers while it is being modulated.

PSD:KM

Test 5-KM – No Flow between Connected Computers over Time

This test verifies that the TOE does not send data to different computers connected to the same interface at different times. Repeat this test for each TOE KM computer port.

Step 1: Configure the TOE and the Operational Environment in accordance with the operational guidance. Connect an authorized peripheral device for each peripheral device type selected in FDP_PDC_EXT.3.1/KM. Connect two computers to a different display and run an instance of a text editor and USB analyzer software on each computer.

Step 2: Connect the first computer to the TOE and ensure it is selected and that no other computers are connected.

Step 3: Exercise the functions of the peripheral device type selected in FDP_PDC_EXT.3.1/KM and verify that the expected results are observed on the selected computer and that the expected traffic is sent and captured using the USB analyzer.

Step 4: Disconnect the first computer. Generate intensive USB HID traffic by moving the mouse at high speed and/or holding down the keyboard space key at the same time.

Step 5: Cease generation of the USB HID traffic, connect the second computer to the same port and ensure it is selected.

Step 6: Verify that no results from the previous use of the peripheral device are observed on the selected computer and that no traffic is sent and captured using the USB analyzer.

Step 7: Reboot the TOE and repeat step 6.

Step 8: Turn off the TOE and repeat step 6.

Step 9: Restart the TOE and repeat step 6.

Step 10: Exercise the functions of the peripheral device type selected in FDP_PDC_EXT.3.1/KM and verify that the expected results are observed on the selected computer and that the expected traffic is sent and captured using the USB analyzer.

For each selectable computer, the evaluator set up two computers per the evaluation activity setup and verified only one computer was connected to the TOE. The evaluator then generated intensive mouse/keyboard data and verified that it was recorded by the connected computer's text editor and USB analyzer. The evaluator then disconnected the first computer and generated HID traffic with no computers connected. The evaluator then connected the second computer in place of the first and observed that no USB activity was captured (i.e., no buffer was emptied), consistent with the TOE properly not retaining and replaying the previous USB traffic. The evaluator repeated the observation after multiple reboots and the TOE being turned off.

PSD:VI
The evaluation shall perform the following tests:

PSD:VI
[TD0539]: Incorrect selection trigger in FTA_CIN_EXT.1.1 in MOD_VI_V1.0
Test 1-VI: Video Source Selection and Identification, TOE Off and Failure States
This test verifies the TOE switching function operates properly and will stop the video output display when in an OFF or FAILURE state.
Step 1: Configure the TOE and the Operational Environment in accordance with the operational guidance.
Step 2: Play a different video with embedded audio on a number of computers for each TOE computer video interface.
Step 3: Connect each computer to a TOE computer video interface.
Step 4: Connect a display to each TOE display interface.
Step 5: Turn on the TOE.
Step 6: For each connected computer, ensure it is selected and verify that the video and its accompanying audio from the selected computer(s) are received on the proper display(s).
Step 7: [Conditional: if *the TOE claims the Combiner Use Case* then] verify that video generated by the TOE has clear identification marking or text to properly identify the source computer shown.
Step 8: Turn off the TOE and verify that no video appears on any connected display.
Step 9: Power on the TOE and cause the TOE to enter a failure state. Verify that the TOE provides the user with a visual indication of failure and that no usable video appears on any connected display.
Step 10: Repeat steps 3 to 9 for each unique display protocol and port type supported by the TOE.

The evaluator configured the connected computers in such a manner that each computer possessed a distinct background that could clearly be distinguished from the other computers. The evaluator turned the TOE on and verified that the TOE displayed the video being sent by the currently selected computer. The evaluator changed the selected computer and verified for each case the correct computer's display was shown. The evaluator turned the TOE off and verified that no video traversed the TOE while the TOE was powered off. The evaluator turned the TOE on and caused the TOE to enter a failure state and ensured that while the TOE was in a failure state other than invalid keyboard/mouse the TOE did not render any video and while in invalid keyboard/mouse the video had a clear indication that an invalid USB device had been connected to the TOE.

The TOE only possesses DisplayPort interfaces and thus is the only port type supported by the TOE.

PSD:VI
Test 2-VI: Computer Video Interface Isolation
[Conditional: perform this test if "switching can be initiated only through express user action" is selected in FDP_SWI_EXT.1.1 in the PSD PP.]
This test verifies that the TOE does not transfer data to any non-selected computer video interface.

Step 1: Configure the TOE and the Operational Environment in accordance with the operational guidance. Connect only the first computer interface cable to one computer. Turn on the TOE.

Step 2: Switch the TOE primary display to computer #1.

Step 3: Observe the primary display to verify that the selected computer is the one that is shown.

Step 4: Remove the non-selected computer video interface cables from the TOE and connect the oscilloscope probe to the TOE #2 computer video interface to verify that no SYNC signal is passed through the TOE. Based on the connection interface protocol, this is performed as follows:

1. Video Graphics Array (VGA) – single ended probe on pins 13 and then 14;
2. High-Definition Multimedia Interface (HDMI) – connect pin 19 to a 3.3V power supply via a 100 Ohm resistor to provide Hot Plug Detect (HPD) signal; Check for signals - differential probe between pins 10 (+) and 12 (-);
3. Digital Visual Interface (DVI)-I – connect pin 16 to a 3.3V power supply via a 100 Ohm resistor to provide HPD signal; Check for signals - single ended probe on pins 8 and C4. Differential probe between pins 23 (+) and 24 (-);
4. DVI-D - connect pin 16 to a 3.3V power supply via a 100 Ohm resistor to provide HPD signal; Check for signals - Differential probe between pins 23 (+) and 24 (-);
5. DisplayPort - connect pin 18 to a 3.3V power supply via 100 Ohm resistor to provide HPD signal; Check for signals - Differential probe between pins 3 (-) and 1 (+) and between 10 (-) and 12 (+);
6. USB Type-C with DisplayPort as Alternate Function – connect pin A8 to a 3.3V power supply via a 100 Ohm resistor to provide HPD signal; Check for signals – Differential probe between pins A2 and A3, A10 and A11; B2 and B3, and B10 and B11.

Step 5: Repeat steps 3 and 4 while selecting other TOE connected computers. Verify that no SYNC signal is present.

Step 6: Repeat steps 3 to 5 with the TOE unpowered. Verify that no SYNC signal is present.

Step 7: With the probe connected to the TOE computer #2 video interface, disconnect / reconnect the computer #1 video cable. Power up the TOE and select computer #1. Attempt to detect the change in the oscilloscope at each one of the TOE #2 computer video interface pins. No changes shall be detected.

Step 8: Repeat step 7 for each one of the other TOE computer video interfaces.

Step 9: Repeat steps 7 and 8, but instead of disconnecting / reconnecting the computer, disconnect and reconnect the display.

Step 10: Repeat steps 7 and 8, but instead of disconnecting / reconnecting the computer, reboot the selected computer.

Step 11: Repeat steps 2 to 10 with each connected computer.

Step 12: [Conditional: if “multiple connected displays” is selected in FDP_CDS_EXT.1.1 then] repeat steps 3 to 10 with each other display connected to the TOE.

Step 13: Repeat this test for each unique display protocol and port type supported by the TOE.

For the claimed video peripheral output protocol (DisplayPort), the evaluator connected a special video connector to the TOE with power to the designated pins and observed the specified pins for each video type. The evaluator then measured the differential between the designated pins, dependent on the supported video protocol, to demonstrate that no SYNC signal is transmitted to a non-selected video port.

The evaluator then turned the TOE off and checked the specified pins again to verify that no SYNC signal traversed the TOE while the TOE was off.

After this, evaluator then connected the same connector to the TOE observed all available pins for the display type. The evaluator performed the specified actions on the selected computer and verified that the observed oscilloscope level was static for each individual pin. This testing was repeated for each combination of ports.

PSD:VI
[TD0514]: Correction to MOD_VI FDP_APC_EXT.1 Test 3 Step 6

[TD0584]: Correction to MOD_VI FDP_APC_EXT.1 Test 3 Step 8, Test 5 Step 11
[TD0686]: DisplayPort CEC Testing Test 3 Step 12

Test 3-VI - Unauthorized Sub-protocols

Note that in the following steps only native video protocol cables shall be used. No conversion from other video protocols is allowed in these tests except as directed in FDP_IPC_EXT.1.1.

This test verifies that unauthorized sub-protocols are blocked.

Perform this test for each of the selections in FDP_PDC_EXT.3.1/VI and FDP_IPC_EXT.1.1.

In the following steps the evaluator shall establish a verified test setup that passes video signals across the TOE.

Step 1: Connect at least one computer with a native video protocol output to the TOE computer #1 video input interface.

Step 2: Connect at least one display with native video protocol to the TOE display output.

Step 3: Power up the TOE and ensure the connected computer is selected.

Step 4: Verify that the video image is visible and stable on the user display.

In the following steps the evaluator shall verify that the test setup properly blocks the unauthorized video sub-protocol traffic.

Step 5: Open the Monitor Control Command Set (MCCS) control console program on the computer and attempt to change the display contrast and brightness. Verify that the display does not change its contrast and brightness accordingly.

Step 6: Disconnect the video cable connecting the display and the TOE and connect the display directly to the *computer*. Verify that the video image is visible and stable on the user display.

Step 7: Attempt to change the display contrast and brightness. Verify that the display does change its contrast and brightness accordingly.

Step 8: Connect the following testing device based on the display video protocol being tested at the peripheral display interface:

- DisplayPort – DisplayPort AUX channel analyzer in series between the display and the TOE
- HDMI~~/DVI-I/ DVI-D~~ – HDMI sink test device
- USB Type-C with DisplayPort as Alternate Function – USB sniffer in series between the display and the TOE
- VGA – VGA sink test device
- DVI-I/DVI-D – DVI sink test device

Step 9: Attempt to change the display contrast and brightness. Verify that the testing device does not capture any MCCS commands.

Step 10: Replace the computer with a source generator for each selected protocol at the computer video interface. If DVI-I or DVI-D is selected, use an HDMI source generator.

Step 11: Collect all 20 EDID file captures, compare them bit-by-bit, and verify that they are all identical excluding null captures recorded in Step 7.

Step 12: [Conditional, if DisplayPort (DP++ - Dual Mode Only), HDMI, or USB Type-C is the selected protocol being tested at the computer video interface, then] run Consumer Electronics Control (CEC) and High-bandwidth Digital Content Protection (HDCP) tests or commands at the generator and verify in the testing device that no CEC or HDCP traffic is captured for HDMI or USB-C, or check for an absence of power on pin 14 (CONFIG2) using an oscilloscope for DisplayPort DP++ Dual Mode.

Step 13: [Conditional, if DVI-D, DVI-I, or HDMI is the selected protocol being tested at the computer video interface, then] run Audio Return Channel (ARC), HDMI Ethernet and Audio Return Channel (HEAC), and HDMI Ethernet Channel (HEC) tests or commands at the generator and verify in the testing device that no ARC, HEAC, or HEC traffic is captured.

Step 14: [Conditional: If *"[HDMI] protocol*" is selected in FDP_IPC_EXT.1.2, then] perform steps 15 and 16 for both pin 13 (CEC) and 14 (UTILITY).

Step 15: Turn off the TOE. Use a multi-meter to measure the resistance-to-ground of the pin at the TOE HDMI peripheral interface and verify it is greater than 2 Mega-ohms.

Step 16: Attach a single ended oscilloscope probe between the pin and the ground, turn on the TOE, and verify that no changes between 0.0v and 0.2v and between 3.0v and 3.3v are detected.

Step 17: [Conditional: if VGA is not the selected protocol being tested, then] disconnect all devices. Connect the display to a TOE computer video interface and the oscilloscope to the TOE display interface in order to verify that no HPD signal is passed by measuring a signal voltage of less than 1.0V. Based on the selected protocol being tested, this is performed as follows:

1. HDMI – connect scope to pin 19 and verify no HPD signal is detected;
2. DVI-D/DVI-I – connect scope to pin 16 and verify no HPD signal is detected;
3. DisplayPort - connect scope to pin 18 and verify no HPD signal is detected;
4. USB Type-C with DisplayPort as Alternate Function – connect scope to pin A8 and B8 and verify no HPD signal is detected.

Step 18: Repeat this test for each of the selections in FDP_PDC_EXT.3.1/VI and FDP_IPC_EXT.1.2.

The evaluator verified that the TOE blocked the MCCS commands by connecting a computer directly and verifying that the computer could control the MCCS commands (brightness and contrast), then connecting the monitor through the TOE and verifying the TOE blocked the MCCS commands and the values could not be changed.

The evaluator verified that other unauthorized sub-protocols are blocked by observing that the TOE blocks HDCP commands and that DisplayPort pin 14 has no voltage.

The evaluator also verified that the HPD signal was not detected.

PSD:VI

[TD0506]: Missing Steps to disconnect and reconnect display

Test 4-VI - Video and EDID Channel Unidirectional Rule

This test verifies that the TOE video path is unidirectional from the computer video interface to the display interface with the exception of EDID, which may be read from the display once at power up and then may be read by the connected computers. The evaluator should have at least two high-resolution displays *of different models* and one low-resolution display for each TOE-supported video protocol.

In the following steps the evaluator should attempt to read display EDID after the TOE completed its self-test / power up. The TOE should not read the new display EDID.

Step 1: Configure the TOE and the Operational Environment in accordance with the operational guidance. Connect a computer and a high-resolution display to the TOE.

Step 2: Ensure the TOE is on, computer #1 is selected, and verify that the display shows video from computer #1 as expected.

Step 3: Turn off the TOE. Disconnect the user display from the TOE.

Step 4: Connect the low-resolution display to the TOE and turn on the TOE *and disconnect the low-resolution display*. After the video is shown on the display, turn off the TOE.

Step 5: Turn on the TOE. After the TOE has completed the self-test, *connect the second high-resolution display of a different model to the TOE*. The TOE may fail to generate video on the user display (i.e., no EDID is read at the TOE power up). If the display is showing video, then run the EDID reading and parsing software on computer #1 and check that there is no active EDID (i.e., the computer is using a default generic display or reading older display settings from the registry).

In the following steps the evaluator shall validate that the TOE video path is unidirectional from the computer video interface to the display interface.

Step 6: Perform steps 7-11 for each TOE computer video interface.

Step 7: Power off the TOE and disconnect the computer #1 video output and the display. Connect the display cable to the TOE computer #1 video interface. Connect the computer #1 video cable to the TOE display interface. This configuration will attempt to force video data through the TOE in the reverse direction.

Step 8: Power up the TOE again.

Step 9: Check that the video is not visible in the display.

Step 10: Perform steps 11 while the TOE is powered on and powered off.

Step 11: Remove the display cable from the TOE and connect the oscilloscope to verify that no SYNC signal is passed through the TOE. Based on the video protocols supported, this is performed as follows:

1. VGA – single ended probe on pins 13 and 14;
2. HDMI – connect pin 19 to a 3.3V power supply via a 100 Ohm resistor to provide HPD signal; Check for signals - differential probe between pins 10 (+) and 12 (-);
3. DVI-I – connect pin 16 to a 3.3V power supply via a 100 Ohm resistor to provide HPD signal; Check for signals - single ended probe on pins 8 and C4. Differential probe between pins 23 (+) and 24 (-);
4. DVI-D - connect pin 16 to a 3.3V power supply via a 100 Ohm resistor to provide HPD signal; Check for signals - Differential probe between pins 23 (+) and 24 (-);
5. DisplayPort - connect pin 18 to a 3.3V power supply via a 100 Ohm resistor to provide HPD signal; Check for signals - Differential probe between pins 3 (-) and 1 (+) and between 10 (-) and 12 (+);
6. 6. USB Type-C with DisplayPort as Alternate Function – connect pin A8 to a 3.3V power supply via a 100 Ohm resistor to provide HPD signal; Check for signals – Differential probe between pins A2 and A3, A10 and A11; B2 and B3, and B10 and B11.

The evaluator verified the TOE does not read the EDID from the connected monitor during power-up or at all. The evaluator connected a different monitor and verified that the EDID value did not change regardless of reboot or connected display changes. The TOE always presented the computer with the same EDID for the board.

The evaluator attempted to send video data through the TOE in the reverse direction and verified the TOE blocked the video. The evaluator also verified that the SYNC signal is not present on the designated pin on the computer port for each of the supported display types when video data is attempted to be forced through the peripheral video port.

PSD:VI

Test 5-VI – No Flow between Connected Computers over Time

This test verifies that the TOE does not send data to different computers connected to the same TOE video interface over time. Repeat this test for each TOE Video port.

Step 1: Configure the TOE and the Operational Environment in accordance with the operational guidance. Run EDID reading and parsing software on two computers and connect a display to the TOE.

Step 2: Connect computer #1 to the TOE, ensure the TOE is on, computer #1 is selected, no other computers are connected, and verify that the display shows video from computer #1 as expected.

Step 3: Capture the TOE EDID content in the software on computer #1 and save as a file with a name that indicates capture time.

Step 4: Disconnect computer #1 and connect an I2C programmer to the same port. Attempt to write the characters “FFFF” over the entire EDID address range.

Step 5: Disconnect the I2C programmer, reconnect computer #1 to the same port, and repeat step 3.

Step 6: Reboot the TOE and repeat step 3.

Step 7: Turn off the TOE and repeat step 3.

Step 8. Restart the TOE and repeat step 3.

Step 9: Disconnect computer #1 and repeat steps 2 to 8 with computer #2 on the same port.

Step 10: Repeat steps 2 to 9 for a total of 20 EDID file captures.

Step 11: Collect all 20 captured EDID files, compare them bit-by-bit, and verify that they are identical.

The evaluator connected a computer to the TOE and observed the current EDID. The evaluator then used a computer with the ability to write to the EDID range and attempted to overwrite the EDID on the TOE. The evaluator observed that the EDID write attempt failed through observing the EDID from the TOE,

rebooting the TOE, and observing the EDID. The evaluator turned the TOE off and observed that there was no EDID on the connected computer. The evaluator turned the TOE on and verified that the original EDID was still presented by the TOE. The evaluator then repeated these steps using different computers until a total of 4 passes had been completed. The evaluator observed the captured EDID values and files and verified that the EDID presented by the TOE did not change at any point in the process.

2.1.1.2 FDP_PDC_EXT.1 Peripheral Device Connection

2.1.1.2.1 TSS Evaluation Activities

The evaluator shall verify that the TSS describes the compatible devices for each peripheral port type supported by the TOE. The description must include sufficient detail to justify any PP-Modules that extend this PP and are claimed by the TOE (e.g., if the ST claims the Audio Input PP-Module, then the TSS shall reference one or more audio input devices as supported peripherals).

Section 6.1.4 of [ST] defines the supported peripheral types as follows:

- Keyboard: purpose-built USB keyboard
- Pointing device:
    - Purpose-built 4-button wired USB trackball
    - Touchscreen (HID pointing interface to one of the two monitors connected to the TOE)
- Video/Display Devices: 2x DisplayPort 1.2 monitors, one of which includes touchscreen capability over a separate USB interface

The evaluator shall verify that the TSS describes the interfaces between the PSD and computers and the PSD and peripherals, and ensure that the TOE does not contain wireless connections for these interfaces.

Section 6.1.4 of [ST] summarizes the TOE external interfaces. This includes peripheral interfaces for keyboard/mouse, and video/display devices. The keyboard/mouse are wired USB 2.0 devices. The video/display devices are wired DisplayPort monitors, one of which also has a wired USB interface. [ST] section 6.1.4 states that the TOE does not authorize any communications with wireless devices. This is further assured by [ST] section 6.1.3, which states that the specific (wired) devices that are authorized to connect to the TOE are set at manufacture time via an allowlist. Any device that is not on the allowlist would not be recognized by the TOE as an authorized device, which would logically preclude the use of wireless devices.

The evaluator shall verify that the list of peripheral devices and interfaces supported by the TOE does not include any prohibited peripheral devices or interface protocols specified in Appendix E.

Appendix E of [PSD PP] defines the following unauthorized devices and protocols:

- USB Mass Storage Device
- Any unauthorized device connected to the PSD through a USB hub
- PS/2

[ST] section 6.1.3 states that USB devices other than those that are bundled with the TOE will not be accepted by the TOE because the allowlist is set at manufacture time to include only those peripherals that are bundled with the TOE by the manufacturer. As this allowlist does not include any devices beyond the keyboard, trackball, and touch panel, the use of USB mass storage devices, USB hubs, and any other USB device in general are unauthorized.

[ST] does not reference PS/2 in its explicit enumeration of supported ports and interfaces and so is assumed not to be supported by the TOE. This is further supported by a schematic port diagram of the TOE (Figure 1) that does not show any PS/2 ports on the device.

The evaluator shall verify that the TSS describes all external physical interfaces implemented by the TOE, and that there are no external interfaces that are not claimed by the TSF.

The evaluator reviewed [ST] and identified that it describes peripheral interfaces for video and USB keyboard/pointing devices (USB trackball and touch panel functionality on DisplayPort monitor connected via separate USB interface). There is no reference to other security-relevant peripheral interface types. The evaluator separately reviewed product documentation (operational guidance, proprietary isolation documentation). In no cases were separate physical interfaces observed to have been omitted from [ST].

PSD:KM
There are no TSS EAs for this component beyond what the PSD PP requires.

N/A

PSD:VI
There are no TSS EAs for this component beyond what the PSD PP requires.

N/A

2.1.1.2.2 Guidance Activities

The evaluator shall verify that the operational user guidance provides clear direction for the connection of computers and peripheral devices to the TOE.

Section 2 of [User] states that the KVM, keyboard, and all associated components are installed in the workstation console at the factory and so no separate installation or configuration actions are required by the user. If it is necessary to remove and replace the KVM, this section includes an itemized list of the KVM connectors, keyboard connectors, power control panel connectors, and console power supply connectors, along with their associated mating cables, so that everything can be reconnected in the proper manner. Figure 1 in section 1 of [User] has a graphic depicting the front panel of the KVM to show its physical ports.

The evaluator shall verify that the operational user guidance provides clear direction for the usage and connection of TOE interfaces, including general information for computer, power, and peripheral devices.

Section 2 of [User] lists all information regarding the specific connections to environmental components. This includes KVM computer and peripheral connections, RS-232 connectivity between the KVM and keyboard remote control, and power connections.

This section also notes, per above, that the TOE is deployed as part of a pre-built system and that it will generally not be necessary for users to modify any physical connections as part of normal operations.

The evaluator shall determine if interfaces that receive or transmit data to or from the TOE present a risk that these interfaces could be misused to import or export user data.

The TOE only supports digital HID and display interfaces. This evaluation activity applies specifically to analog audio interfaces that could be used as a mechanism to covertly transmit data that was not deliberately supplied by a user (e.g. by connecting a microphone to an analog audio output port). No such interfaces exist on the TOE.

The evaluator shall verify that the operational user guidance describes the visual or auditory indications provided to a user when the TOE rejects the connection of a device.

Section 3 of [User] states that if an unauthorized USB device is connected to the TOE, the Invalid KVM VID/PID indicator light is activated, and a message is displayed on the monitor that an invalid USB device was detected.

PSD:KM
The evaluator shall verify that the operational user guidance describes devices authorized for use with the TOE in accordance with the authorized peripheral device connections.

Section 2 of [User] notes that all peripheral devices that are factory-installed in the environmental console in which the TOE is deployed are the only such devices that are to be used with the KVM. In the case of USB devices in particular, the TOE will reject any attempt to use any devices other than those that were installed at the factory.

PSD:VI
The evaluator shall verify that the operational user guidance describes devices authorized for use with the TOE in accordance with the authorized peripheral device connections.

Section 2 of [User] notes that all peripheral devices that are factory-installed in the environmental console in which the TOE is deployed are the only such devices that are to be used with the KVM. With regards to displays in particular, this section notes that the TOE's memory is pre-loaded with the EDID information of the monitors that are included in the console.

2.1.1.2.3 Test Activities

Test 1: The evaluator shall check the TOE and its supplied cables and accessories to ensure that there are no external wired interfaces other than computer interfaces, peripheral device interfaces, and power interfaces.

The evaluator observed the TOE and verified that the TOE only supported acceptable external wired interfaces, USB, Power, and video (DisplayPort).

Test 2: The evaluator shall check the TOE for radio frequency certification information to ensure that the TOE does not support wireless interfaces.

The evaluator examined the TOE design materials and observed no wireless interfaces. The evaluator checked for wireless certifications and found none.

Test 3: The evaluator shall verify that the TOE ports properly reject unauthorized devices and devices with unauthorized protocols as per the Peripheral Device Connections (Appendix E).

For this test, verify device rejection through TOE user indication in accordance with the operational user guidance, an immediate cessation of traffic following device detection or enumeration, or incompatibility of the device interface with the peripheral interface, and through no such device appearing in the real-time hardware information console.

Step 1: Ensure the TOE is powered off. Open a real-time hardware information console on the connected computer.

Step 2: Attempt to connect a USB mass storage device to the TOE peripheral interface.

Step 3: Power on the TOE. Verify the device is rejected.

Step 4: Ensure the USB mass storage device is disconnected, and then attempt to connect it to the TOE peripheral interface again.

Step 5: Verify the device is rejected.

Step 6: Power off the TOE. Connect an unauthorized USB device to a USB hub, and attempt to connect the USB hub to the TOE peripheral interface.

Step 7: Power on the TOE. Verify the device is rejected.

Step 8: Ensure the USB hub is disconnected, and then attempt to connect it to the TOE peripheral interface again.

Step 9: Verify the device is rejected.

Step 10: Power off the TOE. Attempt to connect any Personal System/2 (PS/2) device directly to the TOE peripheral interface.

Step 11: Power on the TOE. Verify the device is rejected.

Step 12: Ensure the PS/2 device is disconnected, and then attempt to connect it directly to the TOE peripheral interface again.

Step 13: Verify the device is rejected.

The evaluator connected a USB mass storage device to the TOE and verified that the TOE rejected the device. The evaluator connected a USB Hub to the TOE and observed that the hub itself was rejected regardless of the USB mass storage device connected. The evaluator verified there are no PS/2 ports on the TOE to connect a PS/2 device to.

PSD:KM

Test 1-KM:

The evaluator shall verify that the TOE ports properly reject unauthorized devices and devices with unauthorized protocols as per the unauthorized peripheral device connections.

For this test, verify device rejection through TOE user indication in accordance with the operational user guidance, an immediate cessation of traffic following device detection or enumeration, no traffic captured on the USB sniffer or analyzer software other than NAK transactions or system messages, or incompatibility of the device interface with the peripheral interface. Also verify device rejection through examination of the USB sniffer or analyzer software for no traffic captured other than NAK transactions or system messages and through examination of the real-time hardware console for no display of new USB devices (recognized or not recognized).

Repeat this test for each keyboard/mouse TOE peripheral interface.

Perform steps 1-6 for each of the following unauthorized devices:

- USB audio headset
- USB camera
- USB printer
- USB user authentication device connected to a TOE keyboard/mouse peripheral interface
- USB wireless LAN dongle

Step 1: Ensure the TOE is powered off and connected to a computer. Run USB analyzer software on the connected computer and connect a USB sniffer to the TOE keyboard/mouse peripheral interface. Open the real-time hardware information console.

Step 2: Attempt to connect the unauthorized device to the USB sniffer.

Step 3: Power on the TOE. Verify the device is rejected.

Step 4: Ensure the unauthorized device is disconnected from the USB sniffer, then attempt to connect it to the USB sniffer again.

Step 5: Verify the device is rejected.

Step 6: Repeat steps 1 through 5 with a USB hub connected between the USB device and USB sniffer and observe that the results are identical.

Step 7: Repeat steps 1-6 with a composite device with non-HID device classes and verify that the non-HID functions are rejected or the entire device is rejected.

The evaluator verified the TOE rejected each of the specified USB devices. The evaluator connected a USB hub to the TOE and observed that the TOE rejected the hub itself regardless of any additional devices connected to the hub.

PSD:KM

Test 2-KM:

The evaluator shall verify that the TOE KM ports do not reject authorized devices and devices with authorized protocols as per the authorized peripheral device connections.

Repeat this test for each of the following four device types:

- Barcode reader;
- Keyboard or Keypad;
- Mouse, Touchscreen, Trackpad, or Trackball; and
- PS/2 to USB adapter (with a connected PS/2 keyboard or mouse).

Step 1: Configure the TOE and the Operational Environment in accordance with the operational guidance. Run an instance of a text editor on a connected computer.

Step 2: Ensure the TOE is powered off.

Step 3: Connect the authorized device to the TOE peripheral interface.

Step 4: Power on the TOE. Verify the TOE user indication described in the operational user guidance is not present.

Step 5: Ensure the connected computer is selected and send inputs using the authorized devices. Verify that the input is received into the text editor or on the screen of the connected computer.

Step 6: Disconnect the authorized device, and then reconnect it to the TOE KM peripheral device interface.

Step 7: Verify the TOE user indication described in the operational user guidance is not present.

Step 8: Send inputs using the authorized devices. Verify that the input is received into the text editor or on the screen of the connected computer.

The TOE does not accept the indicated peripherals because FDP_FIL_EXT.1/KM specifies that the TOE's USB ports have an explicit allow-list that only includes individual devices that are authorized by the vendor during manufacture. This is acceptable because the CC permits the TOE's security functionality to be more restrictive than that described by the SFR. The evaluator observed that the TOE rejected all USB HID peripheral devices that were connected to it aside from those that were explicitly allow-listed by the manufacturer.

PSD:VI

Test 1-VI: The evaluator shall verify that the TOE ports do not reject authorized devices and devices with authorized protocols as per the Peripheral Device Connections appendix in MOD_VI_V1.0.

Repeat this test for each of the selected protocols in FDP_PDC_EXT.3.1/VI:

Step 1: Connect the authorized device with an authorized protocol directly to a computer. Display any image on the device. Disconnect the device from the computer.

Step 2: Configure the TOE and the Operational Environment in accordance with the operational guidance.

Step 3: Ensure the TOE is powered off.

Step 4: Connect the authorized device with an authorized protocol to the TOE peripheral interface.

Step 5: Power on the TOE and verify the TOE user indication described in the operational user guidance is not present.

Step 6: Ensure the connected computer is selected and verify that the device displays the same image as in step 1.

Step 7: Disconnect the authorized device, then reconnect it to the TOE peripheral interface.

Step 8: Verify the TOE user indication described in the operational user guidance is not present.

Step 9: Verify that the device displays the same image as in step 1 and 6.

The evaluator verified that the TOE was able to transmit the video data for DisplayPort, which is the only claimed video output protocol.

2.1.1.3 FDP_RIP_EXT.1 Residual Information Protection

2.1.1.3.1 TSS Evaluation Activity

The evaluator shall verify that the TSS includes a Letter of Volatility that provides the following information:

- Which TOE components have non-volatile memory, the non-volatile memory technology, manufacturer/part number, and memory sizes;
- Any data and data types that the TOE may store on each one of these components;
- Whether or not each one of these parts is used to store user data and how this data may remain in the TOE after power down; and
- Whether the specific component may be independently powered by something other than the TOE (e.g., by a connected computer).

Note that user configuration and TOE settings are not considered user data for purposes of this requirement.

[ST] Appendix A contains the required letter of volatility. The letter covers all types of memory used by the TOE, whether it is volatile or nonvolatile. This description includes the component function of the memory, its component type, manufacturer, and part number, the type of memory (e.g. Flash, SRAM), the size of the memory, whether it handles user data, and if so, what type of user data it handles.

This section also states that all components are powered only by the TOE except those memory components that are part of the environmental keyboard. All volatile memory components of the TOE are purged when the TOE is shut down or reset, while volatile keyboard memory will persist until the system is shut down. As it is not part of the TOE, resetting the TOE will not affect it, but since it shares the same power source as the TOE, shutting down the system will purge it.

The evaluator shall verify that the Letter of Volatility provides assurance that user data is not stored in TOE non-volatile memory or storage.

Appendix A of [ST] identifies that the only user data is keystroke data, which is stored in the volatile memory of the keyboard (which is not part of the TOE), and video and USB HID data. Video and USB HID data are stored in transmitter/receiver CPU DRAM and FPGA runtime memory, all of which are volatile components. All non-volatile memory components are attested not to store user data.

2.1.1.3.2 Guidance Activities

There are no guidance Evaluation Activities for this component.

2.1.1.3.3 Test Activities

There are no test Evaluation Activities for this component.

2.1.1.4 FDP_SWI_EXT.1 PSD Switching

2.1.1.4.1 TSS Evaluation Activity

If the ST includes the selection the “TOE supports only one connected computer”, the evaluator shall verify that the TSS indicates that the TOE supports only one connected computer.

This activity is N/A; [ST] does not include this selection.

If the ST includes the selection "switching can be initiated only through express user action", the evaluator shall verify that the TSS describes the TOE supported switching mechanisms and that those mechanisms can be initiated only through express user action.

Section 6.1.6 of [ST] describes the TOE switching mechanism as toggle buttons on the TOE's wired remote control, which is implemented as a special insert to the connected keyboard that connects to the rest of the TOE through a dedicated channel that is separate from the keyboard USB interface. This section also states that the toggle buttons are only activated if the user also presses the function button on the keyboard, which helps ensure that the switch is engaged deliberately rather than accidentally.

2.1.1.4.2 Guidance Activities

If the ST includes the selection "switching can be initiated only through express user action", the evaluator shall verify that the operational user guidance describes the TOE supported switching mechanisms.

Section 3 of [User] states that switching is performed by pressing the FN (function) key on the keyboard followed by one of the blue toggle buttons that are on the keyboard. This is shown in Figure 4 in the same section, where the four insert buttons are shown on the diagram on the keyboard where the F9 through F12 keys would typically be located, with notations added in the guidance that identify the four buttons as switching to PC1 through PC4, respectively. Note that since PC4 requires the environmental SPARE transmitter to be connected to the TOE, only the first three buttons are relevant to the TSF (per FPT_TST.1, if PC4 is activated while the SPARE module is disconnected, the TOE will return an error as the channel will not be available).

2.1.1.4.3 Test Activities

There are no test Evaluation Activities for this component.

2.1.2 Protection of the TSF (FPT)

2.1.2.1 FPT_FLS_EXT.1 Failure with Preservation of Secure State

This SFR is evaluated in conjunction with FPT_TST.1.

2.1.2.2 FPT_NTA_EXT.1 No Access to TOE

2.1.2.2.1 TSS Evaluation Activity

The evaluator shall examine the TSS to ensure that the TSS documents that connected computers and peripherals do not have access to TOE software, firmware, and TOE memory, except as described above.

Section 6.2.2 of [ST] asserts that the TOE is designed in such a manner that physical and logical access to its internal memory is prevented from unauthorized access, except that connected computers may read video EDID memory.

2.1.2.2.2 Guidance Activities

The evaluator shall check the operational user guidance to ensure any configurations required to comply with this SFR are defined.

The evaluator reviewed [User] and determined that the TOE satisfies this requirement by default and no configuration option exists to affect its behavior.

2.1.2.2.3 Test Activities

There are no test Evaluation Activities for this component.

2.1.2.3 FPT_PHP.1 Passive Detection of Physical Attack

2.1.2.3.1 TSS Evaluation Activity

The evaluator shall verify that the TSS indicates that the TOE provides unambiguous detection of physical tampering of the TOE enclosure and TOE remote controller (if applicable). The evaluator shall verify that the TSS provides information that describes how the TOE indicates that it has been tampered with.

Section 6.2.3 of [ST] describes the TOE's tamper evident seals. The TOE's transmitters, receiver, and optical switch components are all integrated into the same physical chassis. Each transmitter and receiver unit is affixed in the chassis using front and rear tamper evident seals. The optical switch is fixed in the chassis using a metal bar with a screw on each end. Each screw is covered with its own tamper seal. Therefore, no component of the chassis can be removed without the removal of a tamper evident seal. The TOE's wired remote control is physically part of the peripheral keyboard that is bundled with the TOE as part of the integrated workstation. While the keyboard itself is part of the operational environment, it is also closed with tamper seals to prevent undetected access to the remote control embedded in it. In all cases, this section describes the tamper-evident seals as being clearly visible tape with its own serial number and vendor-specific design that would provide evidence of any attempted modification of the TOE.

2.1.2.3.2 Guidance Activities

The evaluator shall verify that the operational user guidance describes the mechanism by which the TOE provides unambiguous detection of physical tampering and provides the user with instructions for verifying that the TOE has not been tampered with.

[User] section 5 describes the tamper-evident seals and provides guidance to the user as to how to detect a broken seal. For those seals that are applied to the chassis, it references figures in the guidance that show where on the chassis the tamper seals are located. This section also states that tamper seals are applied to the underside of the peripheral keyboard.

2.1.2.3.3 Test Activities

Test 1: The evaluator shall verify, for each tamper evident seal or label affixed to the TOE enclosure and TOE remote controller (if applicable), that any attempts to open the enclosure or remove the seal results in the seal being damaged in a manner that is consistent with the operational user guidance.

The evaluator verified that the TOE possessed tamper evident seals and the labels could not be removed without providing any indication that the seal has been tampered. The evaluator verified that when the TOE's housing was tampered with, the TOE provided a visual indication that the device had been tampered with.

Test 2: The evaluator shall verify that it is not possible to administratively disable or otherwise prevent the display of any tampering indicators.

Tampering indicators are based on the physical properties of the tamper seals. This test is not applicable to the TOE because there is no logical mechanism for configuration of the tamper detection mechanism.

2.1.2.4 FPT_TST.1 TSF Testing

2.1.2.4.1 TSS Evaluation Activity

The evaluator shall verify that the TSS describes the self- tests that are performed on start up or on reset (if "upon reset button activation" is selected). The evaluator shall verify that the self-tests cover at least the following:
a) a test of the user interface – in particular, tests of the user control mechanism (e.g., checking that the front panel push-buttons are not jammed); and
b) if "active anti-tamper functionality" is selected, a test of any anti-tampering mechanism (e.g., checking that the backup battery is functional).

[ST] section 6.2.4 describes the power-on and run-time self-tests the TOE performs. The "keyboard KVM selection stuck key test" is the specific test required by part a) of the evaluation activity. This test verifies that the user control mechanism is functional. Part b) is not applicable to the TOE because the TSF does not have active anti-tamper functionality.

The evaluator shall verify that the TSS describes how the TOE ensures a shutdown upon a self-test failure or a failed anti-tampering function, if present. If there are instances when a shutdown does not occur (e.g., a failure is deemed non-security relevant), those cases are identified and a rationale is provided explaining why the TOE's ability to enforce its security policies is not affected.

The TOE does not claim an anti-tampering function (defined by the optional SFR FPT_PHP.3).

The evaluator shall check the TSS to verify that it describes the TOE behavior in case of self-test failure. The evaluator shall verify that the described TOE behavior includes shutting down the PSD functionality once the failure is detected.

[ST] section 6.2.4 identifies a list of specific self-tests and lists the responses to each failed self-test.

Further down the section, a summary is provided of the different types of self-test failures and the TOE's response to each of them, specifically:

- Failures with individual transmitters – a failure of a transmitter-related self-test will have one of three consequences:
    - If the transmitter fails a self-test, the transmitter is disabled, which results in the link being down, and the receiver's failure to communicate with it will be conveyed via status indicator. This prevents the user from selecting the channel associated with the failure, but if other channels do not have this issue, interfaces with those channels are not affected (PSD functionality is shut down for the affected channel).
    - If the link is down between the transmitter and receiver (i.e. physical disconnection), the result is the same as the above without the intermediate step of bringing the link down, since it is already down.
    - In all other failure conditions, the entire TOE is disabled (PSD functionality is shut down for all channels).
- Failures with the receiver – a failure of a receiver-related self-test will cause the TOE to be disabled (PSD functionality is shut down for all channels).
- VID/PID failure – connecting an unauthorized USB device to a USB peripheral port will cause the affected USB port to be disabled, but other ports are not affected by this (PSD functionality is shut down for any communications involving the peripheral port that the unauthorized device was connected to).

- Optical switch failure – the optical switch does not do any logical processing of its own; any opto-mechanical failure will appear to the rest of the TOE as a transmitter link down and will be processed as described above.
- Power distribution board failure – any power-related failures will cause the entire TOE to be non-functional if the receiver or switch is unpowered. If a single transmitter is unpowered, then it will appear to the receiver as if the link is down and so PSD functionality will only be disabled on that channel.
- Failures with the keyboard – the keyboard is part of the TOE's operational environment but it contains the TOE's remote control (which is wired to the TOE over a separate data path from the USB HID channel). Any keyboard self-test failures therefore also disable the remote control, which effectively disables PSD functionality since switching is not possible in this situation.

The evaluator shall examine the TSS to verify that it describes how users verify the integrity of the selections in FPT_TST.1.2 and FPT_TST.1.3. This method can include restarting the TOE, a dedicated self-test, or some other method.

Section 6.2.4 of [ST] states that users can verify the integrity of the TOE by triggering a self-test (e.g., by powering on or rebooting the TOE) and examining the status indicators for self-test failures.

2.1.2.4.2 Guidance Activities

The evaluators shall verify that the operational user guidance describes how users verify the integrity of the selections in FPT_TST.1.2 and FPT_TST.1.3. This method can include restarting the TOE, a dedicated self-test, or some other method.

Section 4 of [User] states that the user can attempt to recover from different types of self-tests based on the type of failure being experienced, as follows:

- KVM failure: for a VID/PID failure, first remove the invalid USB device and then power cycle either the entire system or just the KVM itself. For all other failures, only perform the power cycle step.
- Keyboard: power cycle the entire system (as the keyboard is not covered by a KVM reset operation).
- Power components: in the event of a power-related failure, check the power connection and wiring to the unit.

If any of these remedies fail, replacement of the affected components will be necessary.

2.1.2.4.3 Test Activities

The evaluator shall trigger the conditions specified in the TSS that are used to initiate TSF self-testing and verify that successful completion of the self-tests can be determined by following the corresponding steps in the operational guidance.

The evaluator verified that when the TOE is powered on or reset, the self-tests are performed as evidenced by the Rx fault indicator being active while self-testing is performed, and following self-testing, the light extinguishes and the TOE is active.

2.1.2.5 FPT_TST_EXT.1 TSF Testing

2.1.2.5.1 TSS Evaluation Activity

The evaluator shall check the TSS to verify that it describes the TOE behavior in case of self-test failure. The evaluator shall verify that the described TOE behavior includes shutting down the PSD functionality once the failure is detected.

The functional impact to the TOE of the various possible self-test failures is described under FPT_TST.1 above. With respect to how those failures are visually communicated to the user, per FPT_TST_EXT.1, [ST] section 6.2.4 describes those events as follows:

- Keyboard related failures (e.g. stuck key) – indicated with Keyboard Fault LED
- Unauthorized USB device – indicated with invalid VID/PID LED
- Receiver failure – indicated with Rx Fault LED
- Transmitter failure – indicated with Source Tx Fault LED. Note as there are four transmitters, there are also four lights to correspond with the individual transmitters. It is shown in [User] that the lights are placed above the channel selection buttons on the remote control for the individual transmitters, so that it is obvious which channel the failed transmitter is associated with.

2.1.2.5.2 Guidance Activities

The evaluator shall verify that the operational user guidance:

a) describes how the results of self-tests are indicated to the user
b) provides the user with a clear indication of how to recognize a failed self-test; and
c) details the appropriate actions to be completed in the event of a failed self-test.

The evaluator shall verify that the operational user guidance provides adequate information on TOE self-test failures, their causes, and their indications.

Section 4 of [User] describes what self-tests are performed, what the result of a failed self-test has on the functionality of the TOE, and how that failure is communicated to the user. This section re-iterates the materials in the ST that identify self-test failures causing certain fault LED indicators to light up. It also notes that if a power-related self-test failure occurs, the TOE will simply be inoperable and the user status indicators will not function, in which case the indicators on the power control and supply components would need to be checked to determine the specific electrical or thermal failure trigging the response. If the user experiences such a failure condition, section 4 of [User] includes guidance in various sub-sections as to any corrective actions that may be attempted to resolve the issue.

2.1.2.5.3 Test Activities

The evaluator shall cause a TOE self-test failure and verify that the TOE responds by disabling normal functions and provides proper indications to the user.

The evaluator caused the following self-test failures, that resulted in the following indications and changes in TOE behavior:

- VID/PID fault: the evaluator caused a VID/PID fault by connecting an unauthorized USB device to each peripheral port. When this occurs, the VID/PID Fault light is illuminated, an “invalid USB device” message is displayed on both monitors, and the interface where the fault was caused

does not allow transmission of data, even after reconnecting the valid device. Resetting the TOE with the valid device connected clears the fault.

- Rx fault: the evaluator caused an Rx fault by inverting the connections of two transmitters and then attempting to switch to one of the channels with an incorrect transmitter connected to it. When this occurs, the Rx enters a failure state where the Rx Fault light is illuminated and no communication with a selected computer is possible.
- Tx fault: the evaluator caused a Tx fault in a transmitter by physically disconnecting that transmitter from the receiver. The evaluator verified that the corresponding KVM Source Tx Fault light is illuminated when attempting to select the computer and that switching to that channel is possible but that no video or keyboard/mouse controls work on that specific computer, but that communications with other channels are unaffected.
- Tx fault: the evaluator also caused a Tx fault by connecting a generic network device to a transmitter port. The Rx was not able to recognize the network device as a valid link so a Tx fault was thrown.

2.2 Optional SFRs

No optional SFRs from [PSD PP] are claimed.

2.3 Selection-Based SFRs

2.3.1 User Data Protection (FDP)

2.3.1.1 FDP_SWI_EXT.2 PSD Switching Methods

2.3.1.1.1 TSS Evaluation Activities

The evaluator shall verify that the TSS describes the TOE supported switching mechanisms. The evaluator shall verify that the TSS does not include automatic port scanning, control through a connected computer, and control through keyboard shortcuts as TOE supported switching mechanisms. The evaluator shall verify that the described switching mechanisms can be initiated only through express user action according to the selections.

[ST] section 6.1.6 states that switching is initiated through toggle buttons on the wired remote, which is embedded in the peripheral keyboard (though connects to the rest of the TOE through a data path that is separate from the keyboard's normal USB HID channel).

None of the switching mechanisms involve any of the prohibited behavior (automatic port scanning, control through a connected computer, or control through keyboard shortcuts). Selection buttons are engaged through express user action. In particular, the FN key on the keyboard logically unlocks the ability to use the toggle buttons, functioning similarly to a peripheral guard for the switching mechanism (since the remote control coexists with the user input peripheral). This further assures that the switching occurs through express use because the second button significantly reduces the likelihood that an oblivious user accidentally pushes a toggle button without noticing and will be interacting with the wrong computer once the workstation has their attention again.

PSD:KM
If "peripheral devices using a guard" is selected, the evaluator shall verify that the TSS describes the implementation of the guard function, and verify that multiple, simultaneous express user action is required to switch between connected computers using connected peripheral devices.

N/A; "peripheral devices using a guard" is not selected in FDP_SWI_EXT.2.2.

PSD:UA
There are no TSS EAs for this component beyond what the PSD PP requires.

N/A

2.3.1.1.2 Guidance Activities

The evaluator shall verify that the operational user guidance describes the TOE supported switching mechanisms. The evaluator shall verify that the operational user guidance does not include automatic port scanning, control through a connected computer, and control through keyboard shortcuts as TOE supported switching mechanisms.

Section 3 of [User] identifies how to change the selected computer. As described in the ST, this involves pressing the FN key on the peripheral keyboard and then pressing one of the four selection buttons that are present on the keyboard (which are logically separate from the rest of the keyboard and function as the TOE's remote controller in this case). Pressing the desired selection button will cause the corresponding computer to be selected at which time the peripherals connected to the TOE will begin to interface exclusively with that computer.

The operational user guidance does not include automatic port scanning, control through a connected computer, and control through keyboard shortcuts as TOE supported switching mechanisms. Note for the third item that the TOE does have keyboard-based switching operations but that this is performed using the dedicated remote control keys embedded in the keyboard that interact with the KVM over a separate data path.

PSD:KM
If "peripheral devices using a guard" is selected, the evaluator shall verify that the user guidance describes the steps the user must take as required by the guard to switch between connected computers using a connected peripheral pointing device.

N/A; "peripheral devices using a guard" is not selected in FDP_SWI_EXT.2.2.

2.3.1.1.3 Test Activities

There are no test Evaluation Activities for this component.

N/A

PSD:KM
The evaluator shall ensure that switching is always initiated through express user action using the selected mechanisms throughout testing for FDP_APC_EXT.1 above.
Additional tests for this SFR are performed in FDP_APC_EXT.1 test 1-KM above.

The evaluator verified that all switching of selected computers is the result of user action, and that the user action required to engage a switching operation is consistent with that described in the operational guidance.

2.3.2 TOE Access (FTA)

2.3.2.1 FTA_CIN_EXT.1 Continuous Indications

2.3.2.1.1 TSS Evaluation Activities

The evaluator shall verify that the TSS describes how the TOE behaves on power up and on reset, if applicable, regarding which computer interfaces are active, if any.

Section 6.3.1 of [ST] states that upon successful power on, computer 1 is the default computer if that computer is powered on, computer 2 is the default computer if computer 1 is unpowered, and computer 3 is the default computer if the other two are unpowered. This section also states that when the TOE is reset, the previously selected channel is selected. The environmental keyboard receives power status signals from the computers 1 and 2 which prevent the remote control from being used to select the channels for those computers if they are unpowered. This function does not apply to computer 3 because it has its own independent power supply from the rest of the workstation, per [ST] section 6.1.1.

The evaluator shall verify that the TSS documents the behavior of all indicators when each switching mechanism is in use, and that no conflicting information is displayed by any indicators.

Section 6.3.1 of [ST] states that the transmitter status/channel indicators are located on the top right of the keyboard, with the remote control. When the remote control is engaged to switch the active channel, the light for the corresponding channel turns blue to show it is active. The LNK light for the corresponding transmitter is also illuminated on the TOE chassis.

PSD:VI
There are no TSS EAs for this component beyond what the PSD PP requires.

N/A

2.3.2.1.2 Guidance Activities

The evaluator shall verify that the operational user guidance notes which computer connection is active on TOE power up or on recovery from reset, if applicable. If a reset option is available, use of this feature must be described in the operational user guidance.

[User] section 3 states that after the KVM is booted up during initial power-on, PC1 is the default host computer if it is powered on. If PC1 is powered off, then PC2 is the default computer. If both PC1 and PC2 are powered off, then PC3 is the default computer. This section also states that if the TOE is reset, the selected computer defaults to whatever was selected prior to the reset. [User] section 3 also identifies that the TOE has a reset function and describes how to engage it.

The evaluator shall verify that the operational user guidance documents the behavior of all indicators when each switching mechanism is in use, and that no conflicting information is displayed by any indicators.

[User] section 3 includes a diagram of the keyboard that shows that the channel selection lights are physically embedded in the channel selection buttons on the wired remote control (Figure 4). This section describes how when a given channel is selected, the corresponding light on the selection button will turn on as a blue light. This section also states that the selected channel is indicated through both the keyboard remote control and through LNK lights on the individual transmitters on the TOE chassis itself, but that these are used to communicate the same information.

PSD:VI
There are no guidance EAs for this component beyond what the PSD PP requires.

2.3.2.1.3 Test Activities

Step 1: The evaluator shall configure the TOE and its operational environment in accordance with the operational user guidance.
Step 2: The evaluator shall select a connected computer and power down the TOE, then power up the TOE and verify that the expected selected computer is indicated in accordance with the TSS and that the connection is active.

Step 3: The evaluator shall repeat this process for every possible selected TOE configuration.

Step 4: [Conditional] If "*upon reset button activation*" is selected in FPT_TST.1.1, then the evaluator shall repeat this process for each TOE configuration using the reset function rather than power-down and power-up.

Step 5: The evaluator shall verify that the TOE selected computer indications are always on (i.e., continuous) and fully visible to the TOE user.

Step 6: [Conditional] If the TOE allows peripherals to have active interfaces with different computers at the same time, the evaluator shall verify that each permutation has its own selection indications.

Step 7: [Conditional] If "*a screen with dimming function*" is selected, the evaluator shall verify that indications are visible at minimum brightness settings in standard room illumination conditions.

Step 8: [Conditional] If "*multiple indicators which never display conflicting information*" is selected, the evaluator shall verify that either all indicators reflect the same status at all times, or the indicator for the most recently used switching mechanism displays the correct switching status and that all other indicators display the correct status or no status.

The evaluator verified the following channel selection behavior is enforced by default:

- If computer 1 is powered on, this computer is selected when the TOE is first powered on.
- If computer 1 is powered off and computer 2 is powered on, computer 2 is selected when the TOE is first powered on.
- If both computer 1 and computer 2 are powered off, computer 3 is selected when the TOE is first powered on.
- When the TOE is reset, whatever channel was selected prior the reset remains selected after it.

The evaluator also verified that when a given channel is selected, the active channel is indicated by the blue LED on the corresponding channel selection key on the remote control and by the illuminated green LNK LED on the transmitter corresponding with the active channel.

PSD:VI

Additional testing for this component is performed in test 1-VI of FDP_APC_EXT.1 in section 2.1.1.1.3 above.

3 Security Functional Requirement Evaluation Activities (KM Module)

3.1 Mandatory SFRs

3.1.1 User Data Protection (FDP)

3.1.1.1 FDP_PDC_EXT.2/KM Authorized Devices (Keyboard/Mouse)

3.1.1.1.1 TSS Evaluation Activity

TSS evaluation activities for this SFR are performed under FDP_PDC_EXT.1 above.

Refer to section 2.1.1.2.1 (FDP_PDC_EXT.1) above.

3.1.1.1.2 Guidance Activities

Guidance evaluation activities for this SFR are performed under FDP_PDC_EXT.1 above.

3.1.1.1.3 Test Activities

Testing of this component is performed through evaluation of FDP_PDC_EXT.1 Test 2 as specified in section 2.1.1.2.3 above.

3.1.1.2 FDP_PDC_EXT.3/KM Authorized Connection Protocols (Keyboard/Mouse)

3.1.1.2.1 TSS Evaluation Activity

The evaluator shall examine the TSS and verify it describes which types of peripheral devices that the PSD supports.

Section 6.1.4 of [ST] states that USB 2.0 devices are supported for keyboard and mouse/pointing device. Specifically, the keyboard and trackball are purpose-built USB 2.0 devices. The TOE also has a touchscreen monitor that uses USB 2.0 to communicate the touchscreen activity as a pointing device. This section also states that DisplayPort peripheral video is supported.

The evaluator shall examine the TSS to verify that keyboard or mouse device functions are emulated from the TOE to the connected computer.

[ST] section 6.1.1 states that the keyboard, mouse, and touch panel peripherals are emulated from the TOE to connected computers.

3.1.1.2.2 Guidance Activities

There are no guidance EAs for this component.

3.1.1.2.3 Test Activities

Test activities for this SFR are covered under FDP_APC_EXT.1 tests 1-KM and 3-KM.

3.1.1.3 FDP_UDF_EXT.1/KM Unidirectional Data Flow (Keyboard/Mouse)

3.1.1.3.1 TSS Evaluation Activity

The evaluator shall examine the TSS to verify that it describes if and how keyboard Caps Lock, Num Lock, and Scroll Lock indications are displayed by the TOE and to verify that keyboard internal LEDs are not changed by a connected computer.

[ST] section 6.1.1 indicates that the TOE has caps lock and scroll lock indicators (there is no num lock) embedded in the environmental keyboard. These indicators are considered to be an extension of the TOE because their status is toggled through the RS-232 interface that is used for the embedded remote control and not the USB data path; the TOE does not transmit data to the peripheral keyboard over its USB interface.

The evaluator shall examine the TSS to verify that keyboard and mouse functions are unidirectional from the TOE keyboard/mouse peripheral interface to the TOE keyboard/mouse computer interface.

Section 6.1.1 of [ST] asserts that the TOE routes keyboard/trackball/touch panel data unidirectionally from the attached peripherals to the selected computer.

3.1.1.3.2 Guidance Activities

There are no guidance EAs for this component.

3.1.1.3.3 Test Activities

Test activities for this SFR are covered under FDP_APC_EXT.1 test 3-KM.

3.2 Optional SFRs

3.2.1 User Data Protection (FDP)

3.2.1.1 FDP_FIL_EXT.1/KM Device Filtering (Keyboard/Mouse)

3.2.1.1.1 TSS Evaluation Activity

The evaluator shall examine the TSS and verify that it describes whether the PSD has configurable or fixed device filtering.

Section 6.1.3 of [ST] states that the TOE has fixed device filtration for keyboard, trackball, and touch panel devices. Specifically, it states that the peripherals intended to be used with the TOE are specified at manufacturing time and are permanently allowlisted. No other USB devices are authorized in this manner and will be rejected.

[Conditional - If “configurable” is selected in FDP_FIL_EXT.1.1/KM, then:] the evaluator shall examine the TSS and verify that it describes the process of configuring the TOE for whitelisting and blacklisting KM peripheral devices, including information on how this function is restricted to administrators. The evaluator shall verify that the TSS does not allow TOE device filtering configurations that permit unauthorized devices on KM interfaces.

This is N/A; “configurable” is not selected in FDP_FIL_EXT.1.1/KM.

3.2.1.1.2 Guidance Activities

[Conditional - If “configurable” is selected in FDP_FIL_EXT.1.1/KM, then:] the evaluator shall examine the guidance documentation and verify that it describes the process of configuring the TOE for whitelisting and blacklisting KM peripheral devices and the administrative privileges required to do this.

This is N/A; “configurable” is not selected in FDP_FIL_EXT.1.1/KM.

3.2.1.1.3 Test Activities

Test 1
Perform the test steps in FDP_PDC_EXT.1 with all devices on the PSD KM blacklist and verify that they are rejected as expected.

The evaluator connected a sampling of non-allowlisted devices to the TOE and observed that the TOE rejected these devices in all cases. In this case, rejection is identified by the triggering of the VID/PID Fault light, the lack of recognition of the connected device by the selected computer, and the lack of recognition of the legitimate device, once replaced, until the KVM was reset and the VID/PID fault was cleared.

Test 2
[Conditional: Perform this only if “configurable” is selected in FDP_FIL_EXT.1.1/KM] In the following steps the evaluator shall verify that whitelisted and blacklisted devices are treated correctly.
Step 1: Ensure the TOE and the Operational Environment are configured in accordance with the operational guidance.
Step 2: Connect to the TOE KM peripheral device interface a composite device which contains a HID class and a non-HID class.
Step 3: Configure the TOE KM CDF to whitelist the composite device.
Step 4: Verify that the HID-class part is accepted and that the non-HID class part is rejected through real-time device console and USB sniffer capture, or that the entire device is rejected.
Step 5: Configure the TOE KM CDF to blacklist the device.
Step 6: Verify that both the HID-class part and the non-HID class part is rejected through real-time device console and USB sniffer capture.

This is N/A; “configurable” is not selected in FDP_FIL_EXT.1.1/KM.

3.3 Selection Based SFRs

3.3.1 User Data Protection (FDP)

3.3.1.1 FDP_RIP.1/KM Residual Information Protection (Keyboard Data)

3.3.1.1.1 TSS Evaluation Activity

The evaluator shall verify that the TSS indicates whether or not the TOE has user data buffers.

[ST] section 6.1.5 implies that the TOE has user data buffers for keyboard input because the described reset behavior includes purging keyboard/mouse buffers.

The evaluator shall verify that the TSS describes how all keyboard data stored in volatile memory is deleted upon switching computers.

[ST] section 6.1.5 states that user keyboard data is purged when the TOE is switched to a different computer. Additional details about this mechanism are included in the proprietary isolation document.

3.3.1.1.2 Guidance Activities

There are no guidance EAs for this component.

3.3.1.1.3 Test Activities

There are no test EAs for this component.

3.3.1.2 FDP_SWI_EXT.3 Tied Switching

3.3.1.2.1 TSS Evaluation Activity

The evaluator shall verify that the TSS does not indicate that keyboard and mouse devices may be switched independently to different connected computers.

Section 6.1.6 of [ST] states that all peripherals are tied to the same switch operation such that it is not possible to have different peripherals switched to different computers.

3.3.1.2.2 Guidance Activities

The evaluator shall verify that the guidance does not describe how to switch the keyboard and mouse devices independently to different connected computers.

Section 3 of [User] describes the switching process and is clear with regards to the notion that all peripherals are switched at the same time to the same selected computer using the same operation.

3.3.1.2.3 Test Activities

The evaluator shall verify that the keyboard and mouse devices are always switched together to the same connected computer throughout testing in FDP_APC_EXT.1 in section 2.1.1.1.3 above.

Tests for this SFR are performed in FDP_APC_EXT.1 test 1-KM in section 2.1.1.1.3 above.

Throughout testing, the evaluator observed that any time the input peripherals were in an accepted state (i.e. they were connected to the TOE and no VID/PID fault failure condition was indicated due to a previous rejection of an unauthorized peripheral), the actions taken on those peripherals all affected the selected computer, therefore showing their inputs are tied. This is further confirmed by FDP_APC_EXT.1-KM Test 2 where data flow of KM traffic test tested and observed.

4 Security Functional Requirement Evaluation Activities (VI Module)

4.1 Mandatory SFRs

4.1.1 User Data Protection (FDP)

4.1.1.1 FDP_PDC_EXT.2/VI Authorized Devices (Video Output)

4.1.1.1.1 TSS Evaluation Activity

TSS evaluation activities for this SFR are performed under FDP_PDC_EXT.1 above.

Refer to section 2.1.1.2.1.

4.1.1.1.2 Guidance Activities

Guidance evaluation activities for this SFR are performed under FDP_PDC_EXT.1 above.

4.1.1.1.3 Test Activities

Testing of this component is performed through evaluation of FDP_PDC_EXT.1 as specified in section 2.1.1.2.3 above.

4.1.1.2 FDP_PDC_EXT.3/VI Authorized Connection Protocols (Video Output)

4.1.1.2.1 TSS Evaluation Activity

TSS evaluation activities for this SFR are performed under FDP_PDC_EXT.1 above.

Refer to section 2.1.1.2.1 above.

4.1.1.2.2 Guidance Activities

Guidance evaluation activities for this SFR are performed under FDP_PDC_EXT.1 above.

4.1.1.2.3 Test Activities

Testing of this component is performed through evaluation of FDP_APC_EXT.1 as specified in section 2.1.1.1.3 above.

4.1.1.3 FDP_UDF_EXT.1/VI Unidirectional Data Flow (Video Output)

4.1.1.3.1 TSS Evaluation Activity

There are no TSS EAs for this component.

N/A – no TSS EAs for this component.

4.1.1.3.2 Guidance Activities

There are no guidance EAs for this component.

N/A – no AGD EAs for this component.

4.1.1.3.3 Test Activities

This component is evaluated through evaluation of FDP_APC_EXT.1 as specified in section 2.1.1.1.3 above.

4.2 Optional SFRs

The VI Module does not define any optional SFRs.

4.3 Selection-Based SFRs

4.3.1 User Data Protection (FDP)

4.3.1.1 FDP_CDS_EXT.1 Connected Displays Supported

4.3.1.1.1 TSS Evaluation Activity

The evaluator shall examine the TSS and verify that it describes how many connected displays may be supported at a time.

[ST] section 6.1.2 states that the TOE supports connected displays from a single source video feed (two-head). Based on this, it is clear that it supports two connected displays at a time.

4.3.1.1.2 Guidance Activities

The evaluator shall examine the operational user guidance and verify that it describes how many displays are supported by the TOE.

Section 1 of [User] states that the TOE supports two flat panel display monitors. Figure 1, also in this section, shows two video in ports for each transmitter two video out ports for the receiver, which further reinforces the fact that two displays are supported.

4.3.1.1.3 Test Activities

There are no test EAs for this component beyond what the PSD PP requires.

4.3.1.2 FDP_IPC_EXT.1 Internal Protocol Conversion

4.3.1.2.1 TSS Evaluation Activity

The evaluator shall examine the TSS and verify that it describes how data DisplayPort data is converted.

The TOE accepts TMDS waveform signals at the computer interfaces, per [ST] section 6.1.3. While the physical connectors for the video input interfaces are DisplayPort, the host computers use DisplayPort Dual Mode (DP++) to generate an HDMI signal over this interface. This section states that the input signal is converted to HDMI and then output to the peripheral monitors as DisplayPort, with the AUX channel blocked.

4.3.1.2.2 Guidance Activities

There are no guidance EAs for this component.

N/A – no AGD EAs for this component.

4.3.1.2.3 Test Activities

Testing for this SFR is covered under FDP_APC_EXT.1 Test 3-VI.

4.3.1.3 FDP_SPR_EXT.1/DP Sub-Protocol Rules (DisplayPort Protocol)

4.3.1.3.1 TSS Evaluation Activity

The evaluator shall examine the TSS and verify that it describes that the various sub-protocols are allowed or blocked by the TOE as described by the SFR.

Section 6.1.3 of [ST] states that CEC, HDCP, and MCCS communications are blocked, as is EDID from computer to display. This section also states that there is no direct HPD from display to computer; HPD from the display only goes to the Rx and a separate HPD goes from the Tx to the host computer. There is no mechanism for the TOE to read the EDID from the connected displays because the specific displays connected to the TOE are determined by the vendor during manufacture time and the EDID data is statically inserted into the TOE's memory.

4.3.1.3.2 Guidance Activities

There are no guidance EAs for this component.

N/A – no AGD EAs for this component.

4.3.1.3.3 Test Activities

Testing for this SFR is covered under FDP_APC_EXT.1 Test 3-VI and Test 4-VI.

5 Security Assurance Requirements

5.1 Isolation Document

5.1.1 FDP_APC_EXT.1 Active PSD Connections

The evaluator shall review the Isolation Documentation and Assessment as described in Appendix D of this PP and ensure that it adequately describes the isolation concepts and implementation in the TOE and why it can be relied upon to provide proper isolation between connected computers whether the TOE is powered on or powered off.

The vendor included isolation information in a separate proprietary document ([Isolation]). This document includes design information for the various interfaces, data flows, and operational states in support of how isolation is maintained through these interfaces, for these data flows, and when the TOE is in these states. It also provides design information for how isolation is enforced for the various use cases in which communications are disallowed.

With respect to the requirements from Annex D in the PP, the various sections were found to be satisfied as follows:

- D.1 General: simply summarizes the requirements of the following sections.
- D.2 Design Description: documentation includes physical and logical design information for how isolation is enforced, including visual diagrams for both the TOE physical design and logical data processing flows.
- D.3 Isolation Means Justification:

  The evaluator verified that [Isolation] discusses the following potential unauthorized data flows as being blocked by the TSF:

  - Selected computer to user input peripheral
  - user peripheral output to user peripheral input
  - user peripheral input to user peripheral output
  - user peripheral output to selected computer
  - user peripheral output to non-selected computer
  - connected computers
  - user peripheral input to non-selected computer
  - selected computer to non-selected computer
  - any data to external entities
  - external entities to any TSF data
- D.4 Firmware Dependencies: The Letter of Volatility (Appendix A of [ST]) describes how all of the TOE firmware is handled. Specifically, the TOE firmware is stored on immutable memory that cannot be affected by operational behavior of the TOE. The self-test functionality coupled with the immutability of the firmware storage is sufficient to demonstrate that any catastrophic failure of the firmware will cause the TSF to fail closed and continue to enforce isolation.

PSD:KM

The evaluator shall examine the Isolation Document and verify it describes how the TOE ensures that no data or electrical signals flow between connected computers in both cases (powered on, powered off).

The evaluator verified that [Isolation] describes how no data flows between connected computers.

PSD:VI

The evaluator shall examine the Isolation Document and verify it describes how the TOE ensures that no data or electrical signals flow between connected computers in both cases (powered on, powered off).

The mechanisms by which isolation is enforced between computers is fundamentally the same regardless of the interface type. Therefore, the description in [Isolation] referenced above for keyboard/mouse peripherals is also applicable to video/display peripherals.

5.2 Class ASE: Security Targeted Evaluation

The ST is evaluated as per ASE activities defined in the CEM. In addition, there may be Evaluation Activities specified within Section 5 and the relevant appendices that call for necessary descriptions to be included in the TSS that are specific to the TOE technology type.

No additional evaluation activities are performed for this; refer to sections 2-4 above.

5.3 Class ADV: Development

The design information about the TOE is contained in the guidance documentation available to the end user, the TSS portion of the ST, and in proprietary information contained in documents that is not to be made public (e.g., Isolation Documentation).

5.3.1 ADV_FSP.1 Basic Functional Specification

The functional specification describes the Target Security Functions Interfaces (TSFIs). It is not necessary to have a formal or complete specification of these interfaces. Additionally, because TOEs conforming to this PP will necessarily have interfaces to the Operational Environment that are not directly able to be invoked by TOE users, there is little point specifying that such interfaces be described in and of themselves since only indirect testing of such interfaces may be possible. For this PP, the activities for this family should focus on understanding the interfaces presented in the TSS in response to the functional requirements and the interfaces presented in the AGD documentation. No additional "functional specification" documentation is necessary to satisfy the Evaluation Activities specified.

The interfaces that need to be evaluated are characterized through the information needed to perform the Evaluation Activities listed, rather than as an independent, abstract list.

No additional evaluation activities are performed for this; refer to sections 2-4 above. In particular, the Evaluation Activities for FDP_PDC_EXT.1 and the proprietary Isolation Document are sufficient to identify the security-relevant external interfaces for the TOE.

5.3.1.1 ADV_FSP.1 Evaluation Activity

There are no specific Evaluation Activities associated with these SARs. The Evaluation Activities listed in this PP are associated with the applicable SFRs; since these are directly associated with the SFRs, the tracing element ADV_FSP.1.2D is implicitly already done, and no additional documentation is necessary. The functional specification documentation is provided to support the evaluation activities described in Sections 2-6 and other activities described for AGD, and ATE SARs. The requirements on the content of the functional specification information are implicitly assessed by virtue of the other Evaluation Activities being performed. If the evaluator is unable to perform an activity because there is insufficient interface information, then an adequate functional specification has not been provided.

No additional evaluation activities are performed for this; refer to sections 2-4 above.

5.4 Class AGD: Guidance Documents

The guidance documents will be provided with the ST. Guidance must include a description of how the authorized user verifies that the Operational Environment can fulfill its role for the security functionality. The documentation should be in an informal style and readable by the authorized user.

Guidance must be provided for every operational environment that the product supports as claimed in the ST. This guidance includes:

- Instructions to successfully and securely install the TSF in that environment; and
- Instructions to manage the security of the TSF as a product and as a component of the larger operational environment; and
- Instructions to provide a protected administrative capability.

Guidance pertaining to particular security functionality must also be provided; requirements on such guidance are contained in the Evaluation Activities specified with each requirement.

The evaluators observed that the administrative guidance for the TOE is contained entirely within [User], which includes information on the deployment and usage of the TOE. The TOE is pre-deployed within the purpose-built system that it is deployed as part of; the end customer receives the TOE in a finished and assembled state as part of the workstation in which it is contained. The TOE is therefore deployed in a single operational environment. Section 2 of [User] states that "there is no installation or configuration action required by the user." The TOE also does not provide any administrative capability because it does not claim any conditional requirements for TOE administration.

The security of the TSF is managed through ensuring that the user understands warning indications that are evidence of potential misuse or unintended error states. Section 4 of [User] lists the self-tests that are performed, what a failed self-test means, how that failure is identified to the user, and what actions the user can take to attempt to recover from the failure. Section 5 of [User] identifies to the reader that the TOE has tamper-evident seals, how to identify that a tamper seal was broken, and what action should be taken in the event a broken seal is detected.

5.4.1 AGD_OPE.1 Operational User Guidance

The operational user guidance does not have to be contained in a single document. Guidance to users and Administrators can be spread among documents or web pages. The developer should review the Evaluation Activities contained in Sections 2-6 of this PP to ascertain the specifics of the guidance for which the evaluator will be checking. This will provide the necessary information for the preparation of acceptable guidance.

The evaluator observed that user guidance for setup and operation of the TOE is provided in a single document ([User]).

5.4.1.1 AGD_PRE.1 Preparative Procedures

As with the operational user guidance, the developer should look to the Evaluation Activities contained in Sections 2-6 of this PP to determine the required content with respect to preparative procedures.

This is addressed through the completion of the various guidance evaluation activities in the previous sections.

5.5 Class ALC: Life-Cycle Support

At the assurance level provided for TOEs conformant to this PP, life-cycle support is limited to end-user-visible aspects of the life-cycle, rather than an examination of the TOE vendor's development and configuration management process. This is not meant to diminish the critical role that a developer's practices play in

contributing to the overall trustworthiness of a product; rather, it's a reflection on the information to be made available for evaluation at this assurance level.

5.5.1 ALC_CMC.1 Labeling of the TOE

This component is targeted at identifying the TOE such that it can be distinguished from other products or versions from the same vendor and can be easily specified when being procured by an end user.

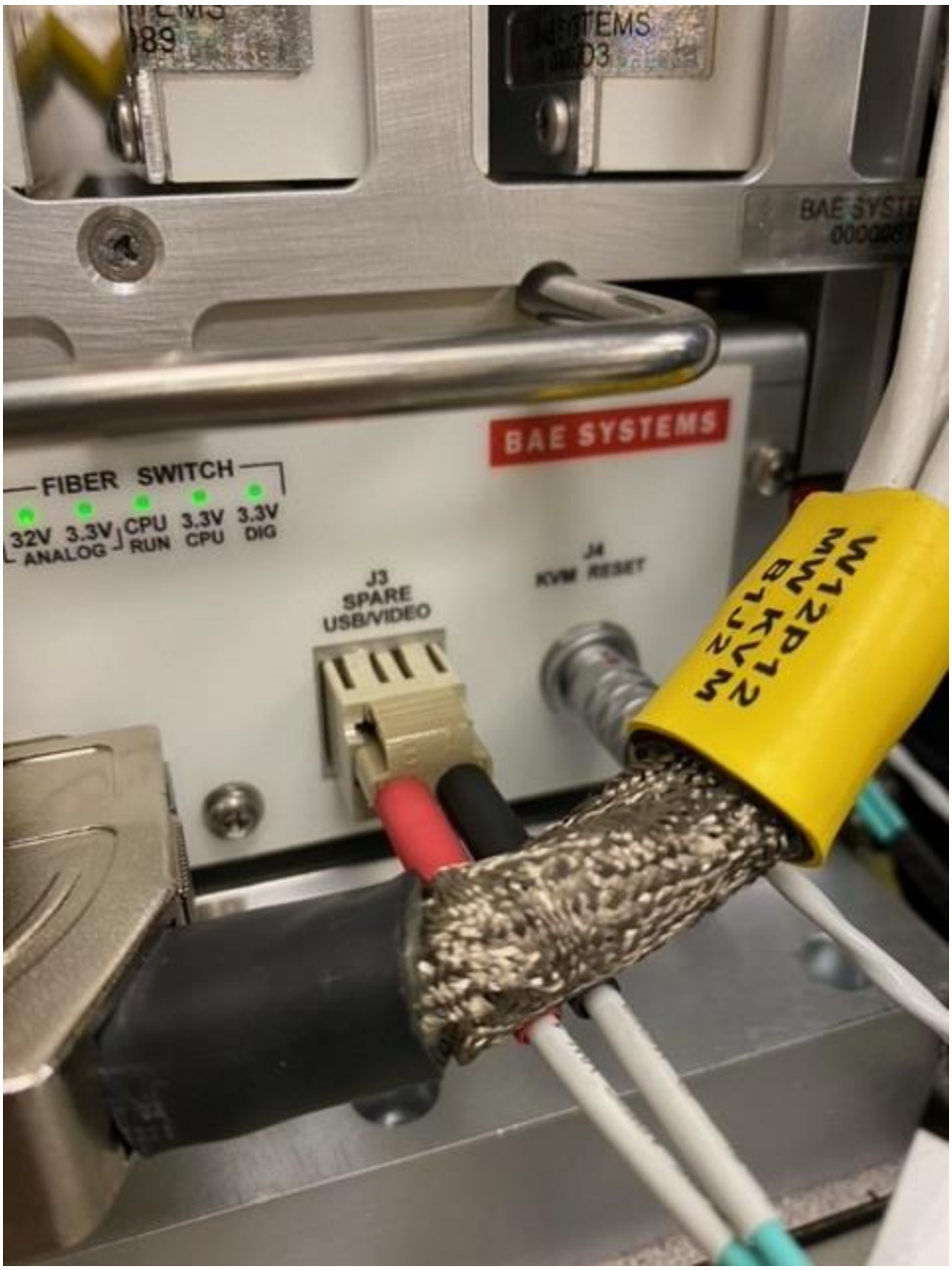
A label should consist of a "hard label" (e.g., stamped into the metal, paper label) or a "soft label" (e.g., electronically presented when queried).

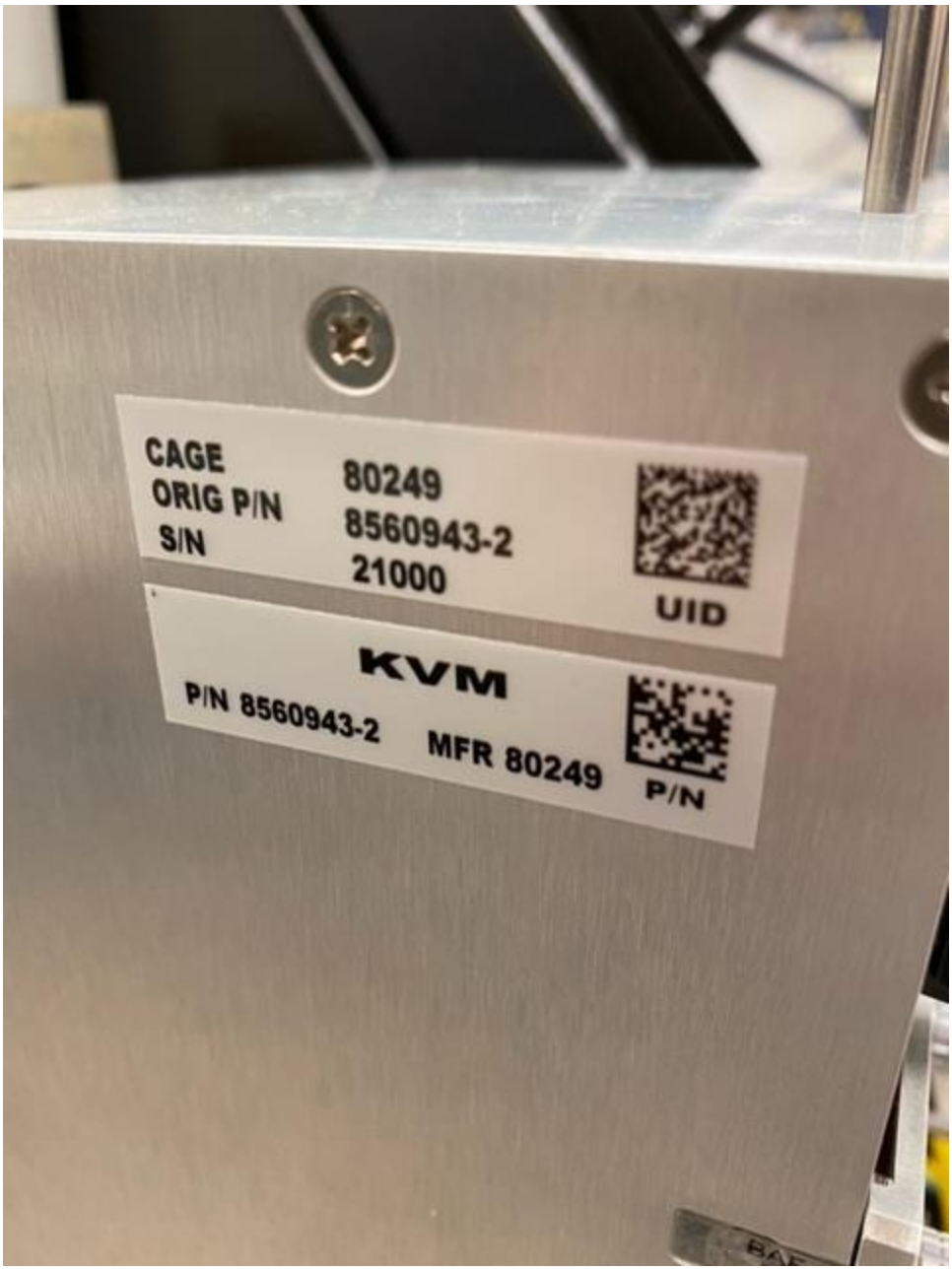
The evaluator performs the CEM work units associated with ALC_CMC.1, as well as the Evaluation Activity specified below.

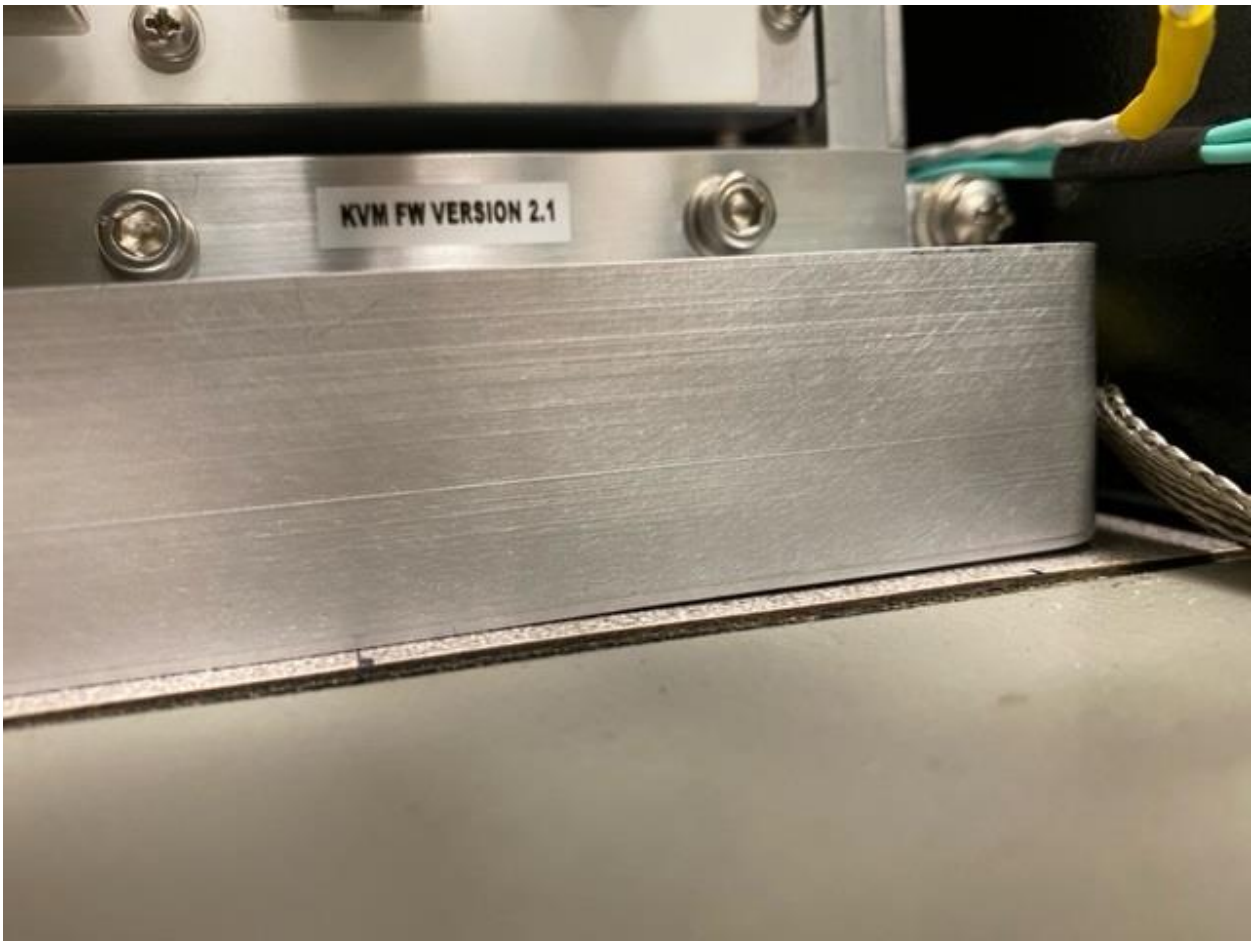
The TOE is a purpose-built device; deployment of the TOE within a larger system will be done as part of the system integration process performed by the customer and TOE developer. Even prior to acquisition, it will be discernable from other vendor products for that reason.

The ST identifies the TOE model and the firmware version number. The TOE is labeled with part number (8560943-2) and firmware version (2.1). The vendor logo is present on the front of the TOE chassis.

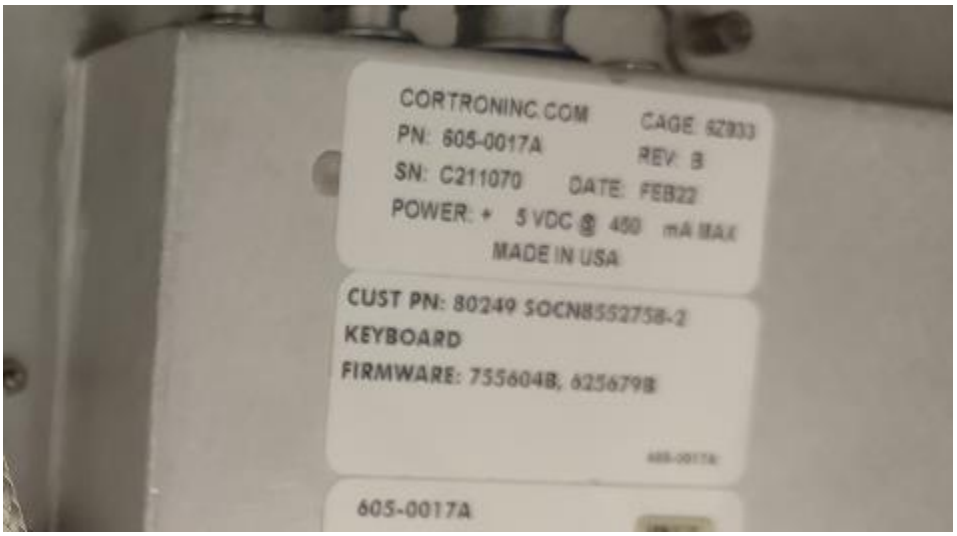
The following pictures show the vendor identifier (front of chassis), part number (top left side of chassis), and firmware identification (front of chassis):


BAE SYSTEMS
FIBER SWITCH
32V ANALOG
3.3V
CPU RUN
3.3V CPU
3.3V DIG
J3
SPARE
USB/VIDEO
J4
KVM RESET


CAGE
80249
ORIG P/N
8560943-2
S/N
21000
UID
KVM
P/N 8560943-2
MFR 80249
P/N



The following label on the keyboard identifies the part number (8552758-2) and firmware version (755604B, 625679B):



5.5.1.1 ALC_CMC.1 Evaluation Activity

The "evaluation evidence required by the SARs" in this PP is limited to the information in the ST coupled with the guidance provided to administrators and users under the AGD requirements. By ensuring that the TOE is specifically identified and that this identification is consistent in the ST and in the AGD guidance, the evaluator implicitly confirms the information required by this component.

Throughout the various documentation references, the evaluators observed that the device model referenced in the operational guidance is consistent with the TOE identified in the ST in terms of physical appearance, product labeling, and claimed functionality.

5.5.2 ALC_CMS.1 TOE CM Coverage

Given the scope of the TOE and its associated evaluation evidence requirements, this component's Evaluation Activities are covered by the Evaluation Activities listed for ALC_CMC.1.

5.6 Class ATE: Tests

Testing is specified for functional aspects of the system as well as aspects that take advantage of design or implementation weaknesses. The former is done through the ATE_IND family, while the latter is through the AVA_VAN family. For this PP, testing is based on advertised functionality and interfaces with dependency on the availability of design information. One of the primary outputs of the evaluation process is the test report as specified in the following requirements.

5.7 ATE_IND Independent Testing – Conformance

Testing is performed to confirm the functionality described in the TSS as well as the guidance documentation. The evaluation activities identify the specific testing activities necessary to verify compliance with the SFRs. The evaluator produces a test report documenting the plan for and results of testing, as well as coverage arguments focused on the platform/TOE combinations that are claiming conformance to this PP.

The evaluator created [Test] to document the test requirements of [PSD PP] and the claimed PP-Modules. This report references external test evidence such as photographs, video recordings, and screen captures that were used to demonstrate that the required testing was performed.

The TOE was delivered to Leidos but was deployed at an alternate site outside the AT&E lab. The evaluators ensured that the physical security of the site was sufficient to ensure the legitimacy of test results per NIAP Labgram 078, with information about the preparation and observation of the site submitted to and subsequently approved by NIAP. Independent testing took place at this alternate site in Columbia, Maryland from August 15, 2022, to October 20, 2022.

The TOE was pre-deployed in mock-up of the workstation in which it will be fielded for operational use.

To allow for the evaluation activities to be performed, the vendor provided the following modifications to the workstation:

- The TOE would generally be located inside the lower portion of the console – it was moved to the physical desktop of the console so that cabling was more readily accessible.
- The TOE ordinarily only authorizes the operation of the USB HID peripherals bundled with the workstation through its fixed device filtration. To perform the unidirectional mouse test, a special build was created to put a Logitech G502 Hero on the allow-list for the tested system.
- The TOE's USB peripheral interfaces use a proprietary physical connector – all USB peripheral cabling included breaks where USB-A male-female connections are used to connect the TOE to each USB peripheral. The evaluator used these to connect other peripheral devices and USB test tools to the TOE.

The workstation includes the following non-TOE components that were used as part of the environment were:

- 2x desktop computers (PSD test systems)
    - OS: Win 10 Pro 20H2, 64 Bit
    - CPU: Intel I3 10100
    - RAM: 8 GB Patriot PS001216
    - SSD: 500 GB NVMe Samsung EVO 970
    - GPU NVIDIA Quadro K420
    - PSU: Corsair CX 450M 450W 80+ Bronze
    - MOBO: MSI H410M Pro
    - Supported Video Types: VGA, DVI x2, HDMI, DP
- 4x rack servers (console systems)
    - Computer 1, computer 2, computer 3:
        - OS: CentOS Linux 8
        - CPU: Intel Xeon E3-1268L
        - RAM: 43 GB DDR3
        - SSD: Samsung EVO 850 mSATA
        - GPU: NVIDIA Quadro M2000
        - Supported Video Types: DP
    - Computer 4 (used for vulnerability testing)
        - Dual Boot
            - OS #1: CentOS Linux 8
            - OS #2: Windows 10 Pro 21H2
        - CPU: Intel Xeon E3-1268L
        - RAM: 43 GB DDR3
        - SSD: Samsung EVO 850 mSATA
        - GPU: NVIDIA Quadro M2000
        - Supported Video Types: DP
- 4 Total Monitors
    - DVI/VGA
        - ASUS VW226 (Quantity: 1)
    - DP/HDMI/DVI
        - Dell U2413F (Quantity:1)
    - Console Monitors (Quantity: 2)
        - AYD Upper
        - AYD Lower-Touch
- BAE Systems “SPARE” Transmitter module, part number 8561040-7
- Keyboard: purpose-built by vendor, part number 8552758-2
- Trackball: purpose-built by vendor, part number 1072378P-5

Additional non-TOE components were used throughout the course of the evaluation. The individual test case will have more information on how each of the testing components were used:

- Lab power supply – Mastech HY3010E S/N 001001010
- Oscilloscope – Agilent Infiniium DSO81004A
- USB Mouse – Logitech G502 Hero

- USB Mouse – Dell Mouse P/N: 0C8639
- USB Keyboard – Targus AKB05UK
- USB Keyboard – Dell L100
- USB Protocol Analyzer – ITIC 1480A USB 2.0 LS/FS/HS
- USB Mass Storage Device – SanDisk 16GB USB 2.0GB
- USB HUB – Sabrent USB Hub
- USB Printer – Canon Prixma IP2820 SN: KKCF48699
- USB Headset – JABRA UC VOICE 550MS S/N 12GA2CO65FC
- USB Smart-card reader – GemPC Twin P/N HWP108760 C
- USB Wireless NIC – ALFA network Long-Rang USB Adapter Model: AWUS036NHR
- USB Barcode Scanner: Symbol DS3508
- USB Camera – ProHT F/#2.0 F:4.8mm
- MCCS Console – SoftMCCS v.2.5.0.1093
- EDID Write Software – EDWriter by ToastyX
- Logitech G Hub Software – version 2022.6.271036
- Keyboard emulator software – Microsoft Windows 10 virtual keyboard
- Google Pixel 4a – Video/Image capture device, running Android 11 IMEI: 357511109902200
- HP 5500 Series Switch JG541A – network device for imposter TX
- 10GBASE-SR SFP+ 850nm 300m DOM Duplex LC MMF Optical Transceiver Module – SFP+ module for Imposter TX network device connection.

The TOE is a single model; all testing was performed on this model.

5.7.1 ATE_IND.1 Evaluation Activity

The evaluator shall prepare a test plan and report documenting the testing aspects of the system. The test plan covers all of the testing actions contained in the CEM and the body of this PP's Evaluation Activities. While it is not necessary to have one test case per test listed in an Evaluation Activity, the evaluator must document in the test plan that each applicable testing requirement in the PP is covered.

The evaluators created [Test] to address all test cases in [PSD PP] and the claimed PP-Modules. The testing is grouped by SFR to show direct correspondence with the required evaluation activities.

The test plan identifies the platforms to be tested, and for those platforms not included in the test plan but included in the ST, the test plan provides a justification for not testing the platforms. This justification must address the differences between the tested platforms and the untested platforms and make an argument that the differences do not affect the testing to be performed. It is not sufficient to merely assert that the differences have no affect; rationale must be provided. If all platforms claimed in the ST are tested, then no rationale is necessary.

No equivalency argument between different device models is made because the TOE is a single device (platform).

The test plan describes the composition of each platform to be tested and any setup that is necessary beyond what is contained in the AGD documentation. It should be noted that the evaluator is expected to follow the AGD documentation for installation and setup of each platform either as part of a test or as a standard pre-test condition. This may include special test equipment or tools. For each piece of equipment or tool, an argument (not just an assertion) should be provided that the equipment or tool will not adversely affect the performance of the functionality by the TOE and its platform.

To the extent that specific external tools are required for testing, these tools are the same as those that are specified in [PSD PP] and the claimed PP-Modules (e.g., oscilloscope, specific types of allowed and

disallowed USB devices, open video cable for channel observation) and therefore no argument is needed that their presence adversely affects the behavior of the TOE.

The evaluator observed that USB cable breaks were necessary in order for test equipment to physically interface with the TOE. These do not affect the performance of the TOE because the existing cabling was simply modified to have standard USB male-female connections be present.

The test plan identifies high-level test objectives as well as the test procedures to be followed to achieve those objectives. These procedures include expected results. The test report (which could just be an annotated version of the test plan) details the activities that took place when the test procedures were executed, and includes the actual results of the tests. This shall be a cumulative account, so if there was a test run that resulted in a failure; a fix installed; and then a successful re-run of the test, the report would show a "fail" and "pass" result (and the supporting details), and not just the "pass" result.

[Test] reproduces the evaluation activities from [PSD PP] and the claimed PP-Modules, each of which include the test objectives, procedures, and expected results in sufficient detail for testing to be reproducible. These activities are written in an implementation-generic manner but are sufficiently detailed for the evaluator to understand the expected steps. For example, the test procedures do not specify a particular method of switching selected channels, but this information was easily discernable to the evaluator through examination of the operational guidance and observation of the TOE itself.

5.8 Class AVA: Vulnerability Assessment

5.8.1 AVA_VAN.1 Vulnerability Survey

For the current generation of this PP, the evaluation lab is expected to survey open sources to discover what vulnerabilities have been discovered in these types of products and in the connected peripherals. In addition, the evaluation lab is expected to survey open sources to discover new vulnerabilities and weaknesses discovered in microcontrollers, ASICs, FPGAs, and microprocessors used in the TOE. In some cases, these vulnerabilities will require sophistication beyond that of a basic attacker. The labs will be expected to comment on the likelihood of these vulnerabilities given the documentation provided by the vendor. This information will be used for the development of future PPs.

The evaluators conducted vulnerability research on the TOE as part of the execution of the AVA_VAN.1 work units. The evaluators did not observe the existence of any general or specialized tools or techniques that are unique to the potential exploitation of peripheral switching functionality. Specifically, no attack techniques related to the following attempted exploits were found, beyond the behavior that is already addressed by the evaluation activities in [PSD PP] and the claimed PP-Modules:

- Attempting to violate security domains by transmitting data from one computer to another.
- Attempting to reverse unidirectional data flow by transmitting data through the TOE in the opposite direction of its intended usage.
- Attempting to exfiltrate data using an unintended mechanism, such as using the TOE's EDID memory to transmit non-EDID data or by using some other TOE interface or variable physical property as a side channel.
- Attempting to use a peripheral to interact with the TOE itself in an unauthorized manner (such as using a USB mass storage device to load modified firmware onto the TOE).
- Attempting to violate device filtration to allow an unauthorized peripheral type to interface with a connected computer through the TOE.

For this device in particular, the TOE has an external interface to a transmitter that is not present in the evaluated configuration by default. This transmitter is implemented as a design requirement from the customer that commissioned the development of the TOE. Per consultation with the validation scheme, this was treated as an external interface to the TOE. Functional testing was performed with this transmitter present to show that peripherals may communicate with it when authorized and that unauthorized data flows are not present (e.g. there is no mechanism to duplicate or misdirect traffic to this interface).

From a vulnerability analysis standpoint, the evaluators also considered the potential ability to manipulate the TOE through this interface. Based on the isolation documentation, the level of attacker sophistication required to send arbitrary communications to the TOE is extremely high, and the memory that can be written to is only the temporary buffer that stores peripheral data; there is no ability to write to any executable memory to alter the behavior of the KVM receiver portion of the TOE. The optical switch portion of the TOE is an opto-mechanical device that does not process data and its functionality therefore cannot be manipulated through the spare transmitter interface. The functional testing of the TOE also observed that a failed connection attempt to a transmitter (e.g. through the transmitter having the wrong unit code for the physical port it was connected to or through connecting a network device that is not recognizable to the TSF) would cause the TOE to enter an appropriate failure state.

5.8.1.1 AVA_VAN.1 Evaluation Activity

As with ATE_IND, the evaluator shall generate a report to document their findings with respect to this requirement. This report could physically be part of the overall test report mentioned in ATE_IND, or a separate document. The evaluator performs a search of public information to determine the vulnerabilities that have been found in peripheral sharing devices and the implemented communication protocols in general, as well as those that pertain to the particular TOE. The evaluator documents the sources consulted and the vulnerabilities found in the report. For each vulnerability found, the evaluator either provides a rationale with respect to its non-applicability, or the evaluator formulates a test (using the guidelines provided in ATE_IND) to confirm the vulnerability, if suitable. Suitability is determined by assessing the attack vector needed to take advantage of the vulnerability. If exploiting the vulnerability requires expert skills and an electron microscope, for instance, then a test would not be suitable and an appropriate justification would be formulated.

The evaluators created [VA] to document the public vulnerability survey that was conducted for the TOE. It was not expected that information would be found regarding this product or any similar product developed by the TOE vendor (e.g., the TOE is a “Gen2” product that is newly-developed, but a “Gen1” product can be assumed to exist) given that the products are purpose-built for specific government customers and are not generally available for commercial sale. The evaluators confirmed that no publicly available information about this product or any previous “Gen1” iteration of the product was found in a general internet search, whether vulnerability-related or not.

The evaluators then conducted a vulnerability search for KVM technologies in general (in case there is some fundamental design flaw in KVM products that would require some mitigation for) as well as for the individual components that are known to be contained within the TOE as disclosed in the letter of volatility.

Searches of public domain sources for potential vulnerabilities in the TOE were conducted multiple times, most recently on January 10, 2023. During each search, no vulnerabilities were revealed that could be exploited by an attacker with Basic attack potential.