

# Mapping Between

## PP-Module for Video/Display Devices, Version 1.0, 19- July-2019

and

## NIST SP 800-53 Revision 5

### Important Caveats

- **Product vs. System.** The Common Criteria is designed for the evaluation of products; the Risk Management Framework (NIST SP 800-37 Revision 2, DOD 8510.01) and associated control/control interpretations (NIST SP 800-53 Revision 5, CNSSI № 1253) are used for the assessment and authorization of mission systems. **Products cannot satisfy controls outside of the system context.** Products may support a system satisfying particular controls, but typically satisfaction also requires the implementation of operational procedures; further, given that systems are typically the product of integration of multiple products configured to meet mission requirements, an overall system assessment is required to determine if the control is satisfied in the overall system context.
- **AC-4.** The primary purpose of a peripheral sharing device is to enforce logical separation between information flows in support of AC-4 generally, and AC-4(21) and AC-4(22) in particular. Any other security controls a peripheral sharing device helps to satisfy is in support of that overarching purpose (i.e. the security requirements are intended to ensure that enforcement of AC-4 and relevant sub-controls cannot be subverted).
- **SA-4(7).** Perhaps it is needless to say, but satisfaction of any NIAP PP supports system satisfaction of SA-4(7), which is the implementation of CNSSP № 11.
- **Limited device functionality.** Peripheral sharing devices are typically isolated from other systems aside from those they are directly connected to. As a result, they generally do not have sophisticated auditing, I&A, or management functionality. For example, a peripheral sharing device's audit mechanism may only have a limited set of records that may only be retrieved on demand; such a device may not meet organizational requirements for automatic logging to a centralized repository. Similarly, a peripheral sharing device's I&A mechanism may be limited to local password-based authentication of a limited number of pre-defined user identities; there should not be an expectation that an organizational user's role and identity are carried over to such a device because a network interface from it to a third-party authentication server may not exist.
- **System context of supported controls.** For a conformant TOE to support these controls in the context of an information system, the selections and assignments completed in the TOE's Security Target must be congruent with those made for the supported controls. For example, the TOE's ability to generate audit records only supports AU-2 to the extent that the TOE's audit records are included in the set of "organization-defined auditable events" assigned by that control. The security control assessor must compare the TOE's functional claims to the behavior required for the system to determine the extent to which the applicable controls are supported.

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
<b>TOE Security Functional Requirements</b>				
FDP_PDC_EXT.2/VI	<u>Peripheral Device Connection (Video Output)</u>	AC-4	<b>Information Flow Enforcement</b>	A conformant TOE supports this control by ensuring that only a well-defined set of authorized peripherals can transfer information to/from computers that are connected to the TOE.
FDP_PDC_EXT.3/VI	<u>Authorized Connection Protocols (Video Output)</u>	AC-4	<b>Information Flow Enforcement</b>	A conformant TOE supports this control by ensuring that only a well-defined set of authorized peripherals can transfer information to/from computers that are connected to the TOE.
FDP_UDF_EXT.1/VI	<u>Unidirectional Data Flow (Video Output)</u>	AC-4(7)	<b>Information Flow Enforcement: One-Way Flow Mechanisms</b>	A conformant TOE supports this control by ensuring that information only transits the TOE in the intended direction.
<b>Optional Requirements</b>				
This PP-Module has no optional requirements.				
<b>Selection-Based Requirements</b>				
FDP_CDS_EXT.1	<u>Connected Displays Supported</u>	N/A	N/A	This SFR does not relate to any security controls; its purpose is to identify the number of distinct video output feeds the TOE has to determine whether the indication of a selected computer requires a video overlay in order to be unambiguous to the user.
FDP_IPC_EXT.1	<u>Internal Protocol Conversion</u>	AC-4	<b>Information Flow Enforcement</b>	A conformant TOE supports this control by requiring any DisplayPort signal received by the TOE to be converted into HDMI in order for its transmission through the TOE to be authorized.
FDP_SPR_EXT.1/DP	<u>Sub-Protocol Rules (DisplayPort Protocol)</u>	AC-4	<b>Information Flow Enforcement</b>	A conformant TOE supports this control by identifying the specific communications that are

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
				allowed and prohibited within a DisplayPort video feed.
FDP_SPR_EXT.1/DVI-D	<u>Sub-Protocol Rules (DVI-D Protocol)</u>	AC-4	<b>Information Flow Enforcement</b>	A conformant TOE supports this control by identifying the specific communications that are allowed and prohibited within a DVI-D video feed.
FDP_SPR_EXT.1/DVI-I	<u>Sub-Protocol Rules (DVI-I Protocol)</u>	AC-4	<b>Information Flow Enforcement</b>	A conformant TOE supports this control by identifying the specific communications that are allowed and prohibited within a DVI-I video feed.
FDP_SPR_EXT.1/HDMI	<u>Sub-Protocol Rules (HDMI Protocol)</u>	AC-4	<b>Information Flow Enforcement</b>	A conformant TOE supports this control by identifying the specific communications that are allowed and prohibited within an HDMI video feed.
FDP_SPR_EXT.1/USB	<u>Sub-Protocol Rules (USB-C Protocol)</u>	AC-4	<b>Information Flow Enforcement</b>	A conformant TOE supports this control by identifying the specific communications that are allowed and prohibited within a USB-C video feed.
FDP_SPR_EXT.1/VGA	<u>Sub-Protocol Rules (VGA Protocol)</u>	AC-4	<b>Information Flow Enforcement</b>	A conformant TOE supports this control by identifying the specific communications that are allowed and prohibited within a VGA video feed.
<b>Objective Requirements</b>				
This PP-Module has no objective requirements.				