Mapping Between

Protection Profile for Peripheral Sharing Switch, Version 3.0, 13-February-2015

and

NIST SP 800-53 Revision 4

Important Caveats

- **Product vs. System.** The Common Criteria is designed for the evaluation of products; the Risk Management Framework (NIST SP 800-37 Revision 1, DOD 8510.01) and associated control/control interpretations (NIST SP 800-53 Revision 4, 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.
- **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.
- **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 4 Control**		**Comments and Observations**
FDP_IFC.1(1)	**Subset Information Control**	AC-4	**Information Flow Enforcement**	A conformant TOE defines a policy for when data flows between specific connected computers and connected peripherals are permitted.

FDP_IFF.1(1)	**Information Control Functions**	AC-4	**Information Flow Enforcement**	A conformant TOE enforces a policy for when data flows between specific connected computers and connected peripherals are permitted.
FDP_IFC.1(2)	**Subset Information Flow Control**	AC-4	**Information Flow Enforcement**	A conformant TOE defines a policy for data flow isolation of peripherals (i.e. data flow is unidirectional and is not authorized when the TOE is unpowered).
FDP_IFF.1(2)	**Simple Security Attributes**	AC-4	**Information Flow Enforcement**	A conformant TOE defines a policy for data flow isolation of peripherals (i.e. data flow is unidirectional and is not authorized when the TOE is unpowered).
FDP_ACC.1	**Subset Access Control**	AC-3	**Access Enforcement**	A conformant TOE defines a policy for the specific types of peripherals that are authorized to transmit data when connected to the TOE.
FDP_ACF.1	**Security Attribute-Based Access Control**	AC-3	**Access Enforcement**	A conformant TOE enforces a policy for the specific types of peripherals that are authorized to transmit data when connected to the TOE.
FDP_RIP.1	**Subset Residual Information Protection**	SC-4	**Information in Shared Resources**	A conformant TOE will have the ability to prevent unintended transfer of information between connected computers.
FPT_PHP.1	**Passive Detection of a Physical Attack**	PE-3(5)	**Physical Access Control:** Tamper Protection	A conformant TOE supports tamper protection by providing a mechanism to detect when tampering has occurred.

		SA-18	**Tamper Resistance and Detection**	A conformant TOE supports enforcement of this control by providing a tamper detection mechanism.
FPT_PHP.3	**Resistance to Physical Attack**	PE-3(5)	**Physical Access Control:** Tamper Protection	A conformant TOE has the ability to protect against tampering by automatically entering a failed state in response to tampering attempts.
FPT_FLS.1	**Failure with Preservation of Secure State**	SC-24	**Fail in Known State**	A conformant TOE will have the ability to enter a secure state (by becoming disabled) in the event of a self-test or anti-tampering failure.
FPT_TST.1	**TSF Testing**	SI-6	**Security Function Verification**	A conformant TOE will run automatic tests to ensure correct operation of its own functionality.
		SI-7	**Software, Firmware, and Information Integrity**	One of the self-tests the TOE must perform is an integrity test of its own software and/or firmware.
FTA_CIN_EXT.1	**Continuous Indications**	N/A	**N/A**	This SFR does not map to any control because this applies to the visual indication of the computer to which it is connected to which is not defined in the controls.
Optional Requirements				
FAU_GEN.1	**Audit Data Generation**	AU-2	**Auditable Events**	A conformant TOE has the ability to generate audit records for various events. The TOE supports the enforcement of the control if its auditable events are consistent with the assignments chosen for the control and if the TOE's audit log is part of the overall system's auditing.

		AU-3	**Content of Audit Records**	A conformant TOE will ensure that audit records include date, type, outcome, and subject identity data. The TOE supports the enforcement of the control if its auditable events are consistent with the assignments chosen for the control and if the TOE's audit log is part of the overall system's auditing.
		AU-3(1)	**Content of Audit Records:** Additional Audit Information	A conformant TOE will generate audit information for some auditable events beyond what is mandated in AU-3. This may or may not be sufficient to satisfy this control based on the additional audit information required by the organization. The TOE supports the enforcement of the control if its auditable events are consistent with the assignments chosen for the control and if the TOE's audit log is part of the overall system's auditing.
		AU-12	**Audit Generation**	A conformant TOE has the ability to generate audit logs. The TOE supports the enforcement of the control if its auditable events are consistent with the assignments chosen for the control and if the TOE's audit log is part of the overall system's auditing.
FIA_UAU.2	**User Authentication Before Any Action**	AC-14	**Permitted Actions Without Identification of Authentication**	A conformant TOE will require user identification and authentication to

				perform any management activity.
		IA-2	**Identification and Authentication (Organizational Users)**	A conformant TOE will provide a mechanism to identify and authenticate organizational users attempting to administer the TOE. Note however that the TOE's authentication mechanism isn't necessarily linked to an organization-wide repository of user identity and credential data.
FIA_UID.2	**User Identification Before Any Action**	AC-14	**Permitted Actions Without Identification of Authentication**	A conformant TOE will require user identification and authentication to perform any management activity.
		IA-2	**Identification and Authentication (Organizational Users)**	A conformant TOE will provide a mechanism to identify and authenticate organizational users attempting to administer the TOE. Note however that the TOE's authentication mechanism isn't necessarily linked to an organization-wide repository of user identity and credential data.
FMT_MOF.1	**Management of Security Functions Behavior**	AC-3	**Access Enforcement**	A conformant TOE will not permit management of configurable device filtration (CDF) unless proper authorization is provided.
		AC-3(7)	**Access Enforcement:** Role-Based Access Control	A conformant TOE will restrict access to management functionality to members of a certain role.

		AC-6	**Least Privilege**	A conformant TOE enforces least privilege by restricting the users that are able to perform management functionality.
FMT_SMF.1	**Specification of Management Functions**	CM-6	**Configuration Settings**	A conformant TOE may satisfy one or more capabilities defined in this SFR. In general, a conformant TOE will satisfy this control to the extent that the TOE provides a method to configure its behavior in accordance with organizational requirements. Specific additional controls may be supported depending on the functionality claimed by the TOE.
FMT_SMR.1	**Security Roles**	AC-2 (7)	Account Management: Role-Based Schemes	A conformant TOE has the ability to associate users with roles, in support of part a of the control.
Selection-Based Requirements				
FTA_ATH_EXT.1	**User Authentication Device Reset**	SC-4	**Information in Shared Resources**	A conformant TOE will support the enforcement of this control by ensuring that a connected authentication device peripheral will not unintendedly communicate with a connected computer.
FTA_ATH_EXT.2	**User Authentication Device Session Termination**	AC-12	**Session Termination**	A conformant TOE will terminate all active sessions when one session is terminated or when the TOE becomes unpowered.