Mapping Between

Protection Profile for Hardcopy Devices, Version 1.0, 10-September-2015 and Protection Profile for Hardcopy Devices – v1.0, Errata #1, June 2017

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.
- **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 5 Control Supports**		**Comments and Observations**
Mandatory Requirements				
FAU_GEN.1	**Audit Data Generation**	AU-2	**Event Logging**	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

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
				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 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-12	**Audit Record Generation**	A conformant TOE has the ability to generate audit logs. The TOE supports the enforcement of parts (a) and (c) 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. Part (b) is not satisfied by a conformant TOE because the PP does not define functionality to suppress/enable the generation of specific audit records (which would typically be expressed in CC as FAU_SEL.1).
FAU_GEN.2	**User Identity Association**	AU-3	**Content of Audit Records**	A conformant TOE will ensure that audit records

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
				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.
FAU_STG_EXT.1	**External Audit Trail Storage**	AU-4(1)	**Audit Log Storage Capacity:** Transfer to Alternate Storage	A conformant TOE has the ability to logically transmit audit data to a location in its Operational Environment. While this SFR requires the TSF to store generated audit data on the TOE, a minimum storage size or retention period is not specified. Therefore, a TOE may support the enforcement of this control if the local storage of audit data is limited or transitory.
		AU-9(2)	**Protection of Audit Information:** Store on Separate Physical Systems or Components	A conformant TOE must be able to transmit audit data to a logically remote location. It can be used to support the enforcement of this control if the recipient of the audit data is physically remote from the TOE.
FCS_CKM.1(b)	**Cryptographic Key Generation (Symmetric Keys)**	SC-12	**Cryptographic Key Establishment and Management**	The ability of the TOE to generate asymmetric keys satisfies the key generation portion of this control.
		SC-12(2)	**Cryptographic Key Establishment and Management:** Symmetric Keys	A conformant TOE ensures that generated symmetric keys provide an appropriate level of security.
FCS_CKM_EXT.4	**Cryptographic Key Material Destruction**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE has the ability to securely destroy cryptographic keys through either its own mechanisms or environmental ones.

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
FCS_CKM.4	**Cryptographic Key Destruction**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE has the ability to securely destroy cryptographic keys through either its own mechanisms or environmental ones.
FCS_COP.1(a)	**Cryptographic Operation (Symmetric Encryption/Decryption)**	SC-13	**Cryptographic Protection**	A conformant TOE has the ability to perform (or invoke environmental methods to perform) symmetric encryption using NSA-approved and FIPS-validated algorithms.
FCS_COP.1(b)	**Cryptographic Operation (for Signature Generation/Verification)**	SC-13	**Cryptographic Protection**	A conformant TOE has the ability to perform (or invoke environmental methods to perform) cryptographic signature operations using NSA-approved and FIPS-validated algorithms.
FCS_RBG_EXT.1	**Cryptographic Operation (Random Bit Generation)**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE has the ability to generate (or invoke environmental methods to generate) random bits for use in cryptographic services using FIPS- and NSA-approved standards.
FDP_ACC.1	**Subset Access Control**	AC-3	**Access Enforcement**	A conformant TOE defines an access control policy that is used to enforce access restrictions on user data under the control of the TSF.
FDP_ACF.1	**Security Attribute Based Access Control**	AC-3	**Access Enforcement**	A conformant TOE implements an access control policy that is used to enforce access restrictions on user data under the control of the TSF.
FIA_AFL.1	**Authentication Failure Handling**	AC-7	**Unsuccessful Logon Attempts**	The TOE has the ability to detect when a defined number of unsuccessful authentication attempts occurs and take some corrective action.
FIA_ATD.1	**User Attribute Definition**	AC-2	**Account Management**	A conformant TOE supports the enforcement of this control by maintaining user

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
				attributes that may be configured in accordance with organizational policy.
		IA-2	**Identification and Authentication (Organizational Users)**	A conformant TOE supports the enforcement of this control by defining user attributes that are used in support of identification and authentication to the TOE.
FIA_PMG_EXT.1	**Password Management**	IA-5(1)	**Authenticator Management:** Password-Based Authentication	A conformant TOE will have the ability to enforce some minimum password complexity requirements.
FIA_UAU.1	**Timing of Authentication**	AC-14	**Permitted Actions Without Identification or Authentication**	A conformant TOE will define a list of actions that are permitted prior to authentication.
		IA-2 - or - IA-8	**Identification and Authentication (Organizational Users)** **- or -** **Identification and Authentication (Non-Organizational Users)**	A conformant TOE has the ability to require that certain functions require successful authentication to access. Whether IA-2, IA-8, or both controls apply is dependent on whether the TOE supports external authentication of organizational users (e.g. LDAP, Kerberos, Active Directory), implements its own local authentication for non-organizational users, or both.
FIA_UAU.7	**Protected Authentication Feedback**	IA-6	**Authentication Feedback**	The TOE is required to provide obscured feedback to the user while authentication is in progress.
FIA_UID.1	**Timing of Identification**	AC-14	**Permitted Actions Without Identification or Authentication**	A conformant TOE will define a list of actions that are permitted prior to identification.
		IA-2	**Identification and Authentication (Organizational Users)**	A conformant TOE has the ability to require that certain functions require successful identification to access.
FIA_USB.1	**User-Subject Binding**	AC-16(3)	**Security and Privacy Attributes:** Maintenance of	A conformant TOE supports the enforcement of this control by associating users

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
			Attribute Associations by System	with subject data such that the TSF is able to enforce appropriate access control policies based on the authenticated user.
FMT_MOF.1	**Management of Security Functions Behavior**	AC-3	**Access Enforcement**	A conformant TOE supports this control by providing access control restrictions to various functions. Note that the extent of support depends on the extent to which this behavior is captured in the organizational access control policies defined by AC-1.
		AC-3(7)	**Access Enforcement:** Role-Based Access Control	A conformant TOE supports this control by providing role-based level of management functionality to administrators.
		AC-6	**Least Privilege**	A conformant TOE supports the concept of least privilege by limiting device management functions to only the roles that are needed to perform them.
		AC-6(1)	**Least Privilege:** Authorize Access to Security Functions	A conformant TOE will enforce access restrictions such that users are not granted excessive administrative privileges to manage the TSF.
		AC-6(10)	**Least Privilege:** Prohibit Non-Privileged Users from Executing Privileged Functions	A conformant TOE supports this control by defining some management functionality as privileged such that ordinary users cannot perform these functions.
FMT_MSA.1	**Management of Security Attributes**	AC-2	**Account Management**	A conformant TOE assigns group and role memberships for access authorizations.
		AC-3(7)	**Access Enforcement:** Role-Based Access Control	A conformant TOE supports the enforcement of this control by authorizing the management of user security attributes on a per-role basis.

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
		AC-16(2)	**Security and Privacy Attributes:** Attribute Value Changes by Authorized Individuals	A conformant TOE supports the enforcement of this control by enforcing access restrictions on the subjects that are authorized to modify attribute data.
FMT_MSA.3	**Static Attribute Initialization**	AC-16(2)	**Security and Privacy Attributes:** Attribute Configuration by Authorized Individuals	A conformant TOE supports the enforcement of this control by enforcing restrictions on the subjects that are authorized to change the default values of attribute data.
FMT_MTD.1	**Management of TSF Data**	AC-3	**Access Enforcement**	A conformant TOE will not permit manipulation of its stored TSF and configuration data 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 manage TSF data.
FMT_SMF.1	**Specification of Management Functions**	CM-6	**Configuration Settings**	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. However, this depends on the extent to which organizational requirements align with the claimed management functions. Specific additional controls may be supported depending on the functionality claimed by the TOE.
FMT_SMR.1	**Security Roles**	AC-2(7)	**Account Management:** Privileged User Accounts	A conformant TOE defines a role-based access model that allows individual users to be assigned to different administrative roles.

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
		AC-3(7)	**Access Enforcement:** Role-Based Access Control	A conformant TOE has the ability to enforce differing levels of access control to individual management roles.
FPT_SKP_EXT.1	**Protection of TSF Data**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE supports the enforcement of this control by protecting stored pre-shared keys, symmetric keys, and private keys.
FPT_STM.1	**Reliable Time Stamps**	AU-8	**Time Stamps**	A conformant TOE can generate or use time stamps to address the actions defined in this control.
		SC-45(1)	**System Time Synchronization:** Synchronization with Authoritative Time Source	A conformant TOE may have the ability to synchronize with an NTP server in its operational environment, satisfying this control.
FPT_TST_EXT.1	**TSF Testing**	SI-6	**Security and Privacy 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 may perform is an integrity test of its own software or firmware.
		SI-7(1)	**Software, Firmware, and Information Integrity:** Integrity Checks	One of the self-tests the TOE may perform is an integrity test of its own software or firmware.
FPT_TUD_EXT.1	**Trusted Update**	CM-14	**Signed Components**	A conformant TOE requires that TOE updates include integrity measures using a digital signature and optional published hash.
		SI-7(1)	**Software, Firmware and Information Integrity:** Integrity Checks	A conformant TOE has the ability to verify the integrity of updates to it.
FTA_SSL.3	**TSF-Initiated Termination**	AC-2(5)	**Account Management:** Inactivity Logout	A conformant TOE will have the ability to log out after a period of inactivity.
		AC-12	**Session Termination**	A conformant TOE will have the ability to terminate an

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
				idle remote interactive session.
FTP_ITC.1	**Inter-TSF Trusted Channel**	IA-3(1)	**Device Identification and Authentication:** Cryptographic Bidirectional Authentication	A conformant TOE may support the enforcement of this control if the protocol(s) used to establish trusted communications uses mutual authentication.
		SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE has the ability to ensure the confidentiality and integrity of information transmitted between the TOE and another trusted IT product.
		SC-8(1)	**Transmission Confidentiality and Integrity:** Cryptographic Protection	The TOE supports a cryptographic method of protecting data in transit.
FTP_TRP.1(a)	**Trusted Path (for Administrators)**	IA-3(1)	**Device Identification and Authentication:** Cryptographic Bidirectional Authentication	A conformant TOE may support the enforcement of this control if the protocol(s) used to establish trusted communications uses mutual authentication.
		SC-8(1)	**Transmission Confidentiality and Integrity:** Cryptographic Protection	A conformant TOE will have the ability to prevent unauthorized disclosure of information and detect modification to that information.
		SC-11	**Trusted Path**	The TOE establishes a trusted communication path between remote administrators and itself.
FTP_TRP.1(b)	**Trusted Path (for Non-Administrators)**	IA-3(1)	**Device Identification and Authentication:** Cryptographic Bidirectional Authentication	A conformant TOE may support the enforcement of this control if the protocol(s) used to establish trusted communications uses mutual authentication.
		SC-8(1)	**Transmission Confidentiality and Integrity:** Cryptographic Protection	A conformant TOE will have the ability to prevent unauthorized disclosure of information and detect modification to that information.

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
		SC-11	**Trusted Path**	The TOE establishes a trusted communication path between remote users and itself.
Conditionally Mandatory Requirements				
FPT_KYP_EXT.1	**Protection of Key and Key Material**	AC-20(2)	**Use of External Systems:** Portable Storage Devices – Restricted Use	A conformant TOE supports the enforcement of this control by enforcing usage limitations on removable storage devices.
		SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE will ensure that secret key and keying material data are not stored in plaintext except in specific cases where appropriate.
		SC-28(3)	**Protection of Information at Rest:** Cryptographic Keys	A conformant TOE will ensure that its cryptographic keys are protected at rest using an appropriate method.
FCS_KYC_EXT.1	**Key Chaining**	SC-12	**Cryptographic Key Establishment and Management**	The ability of a conformant TOE to maintain a key chain satisfies the key access portion of this control.
		SC-28(3)	**Protection of Information at Rest:** Cryptographic Keys	A conformant TOE will ensure that its cryptographic keys are protected at rest using an appropriate method.
FDP_DSK_EXT.1	**Protection of Data on Disk**	SC-28	**Protection of Information at Rest**	The primary purpose of the TOE is to ensure that data at rest is protected against unauthorized access.
		SC-28(1)	**Protection of Information at Rest:** Cryptographic Protection	A conformant TOE will encrypt data at rest using AES.
FDP_FXS_EXT.1	**Fax Separation**	AC-3	**Access Enforcement**	A conformant TOE enforces this control on the TOE's fax interface by defining authorized usage for this interface and ensuring that it can only be used for an authorized function.

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
		SC-3(2)	**Security Function Isolation:** Access and Flow Control Functions	A conformant TOE supports enforcement of this control by logically separating the fax interface from non-fax uses.
Optional Requirements				
FAU_SAR.1	**Audit Review**	AU-7	**Audit Record Reduction and Report Generation**	A conformant TOE provides audit review mechanisms to administrators.
FAU_SAR.2	**Restricted Audit Review**	AU-9(6)	**Protection of Audit Information:** Read-Only Access	A conformant TOE supports the enforcement of this control by enforcing read-only access to IPS records to authorized subjects.
FAU_STG.1	**Protected Audit Trail Storage**	AU-9	**Protection of Audit Information**	A conformant TOE has the ability to prevent unauthorized modification and deletion of audit records.
		AU-9(6)	**Protection of Audit Information:** Read-Only Access	A conformant TOE has the ability to prevent unauthorized modification and deletion of audit records. If the TOE prevents this by preventing all modification and deletion of audit records (i.e., there is no 'authorized' ability to do this), it can be used to support the enforcement of this control.
FAU_STG.4	**Prevention of Audit Data Loss**	AU-5	**Response to Audit Logging Process Failures**	A conformant TOE has the ability to react in a specific manner when the allocated audit storage space is full. This SFR does not require the TOE to generate an alert when this occurs so only part (b) of the control is satisfied.
FCS_CKM.1(a)	**Cryptographic Key Generation (for asymmetric keys)**	SC-12	**Cryptographic Key Establishment and Management**	The ability of the TOE to generate asymmetric keys satisfies the key generation portion of this control.
		SC-12(3)	**Cryptographic Key Establishment and**	A conformant TOE ensures that generated asymmetric

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
			Management: Asymmetric Keys	keys provide an appropriate level of security.
FDP_RIP.1(a)	**Subset Residual Information Protection**	SC-4	**Information in Shared Resources**	A conformant TOE supports this control by ensuring that any previous information content of a resource is made unavailable by overwriting data upon the deallocation of the resource.
FDP_RIP.1(b)	**Subset Residual Information Protection**	SC-4	**Information in Shared Resources**	A conformant TOE supports this control by ensuring that any previous information content of a resource is made unavailable by overwriting data upon the request of an administrator.
Selection-Based Requirements				
FCS_COP.1(c)	**Cryptographic operation (Hash Algorithm)**	SC-13	**Cryptographic Protection**	A conformant TOE has the ability to perform hashing using NSA-approved and FIPS-validated algorithms.
FCS_COP.1(d)	**Cryptographic Operation (AES Data Encryption/Decryption)**	SC-13	**Cryptographic Protection**	A conformant TOE has the ability to perform AES encryption and decryption using NSA-approved and FIPS-validated algorithms.
FCS_COP.1(e)	**Cryptographic Operation (Key Wrapping)**	SC-13	**Cryptographic Protection**	A conformant TOE has the ability to perform key wrapping using NSA-approved and FIPS-validated algorithms.
FCS_COP.1(f)	**Cryptographic Operation (Key Encryption)**	SC-13	**Cryptographic Protection**	A conformant TOE has the ability to perform key encryption-using NSA-approved and FIPS-validated algorithms.
FCS_COP.1(g)	**Cryptographic Operation (for Keyed-Hash Message Authentication)**	SC-13	**Cryptographic Protection**	A conformant TOE has the ability to perform keyed-hash message authentication using NSA-approved and FIPS-validated algorithms.

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
FCS_COP.1(h)	**Cryptographic Operation (for Keyed-Hash Message Authentication)**	SC-13	**Cryptographic Protection**	A conformant TOE has the ability to perform keyed-hash message authentication using NSA-approved and FIPS-validated algorithms.
FCS_COP.1(i)	**Cryptographic Operation (Key Transport)**	SC-13	**Cryptographic Protection**	A conformant TOE has the ability to perform key transport using NSA-approved and FIPS-validated algorithms.
FCS_HTTPS_EXT.1	**HTTPS-Selected**	IA-5(2)	**Authenticator Management:** Public Key-Based Authentication	A conformant TOE may support the implementation of PKI-based authentication by validating peer certificates as part of the authentication process.
		SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE has the ability to ensure the confidentiality and integrity of information transmitted between the TOE and another trusted IT product.
		SC-8 (1)	**Transmission Confidentiality and Integrity:** Cryptographic Protection	The TOE supports a cryptographic method of protecting data in transit.
		SC-13	**Cryptographic Protection**	The TOE provides cryptographic methods to secure data in transit, which may satisfy organization-defined uses if the functionality claimed by the TSF is consistent with organizational requirements.
FCS_IPSEC_EXT.1	**IPsec Selected**	IA-5(2)	**Authenticator Management:** Public Key-Based Authentication	A conformant TOE implements peer authentication for IPsec.
		SC-7(5)	**Boundary Protection:** Deny by Default - Allow by Exception	A conformant TOE's IPsec implementation includes a default-deny posture in its SPD.

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
		SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE implements IPsec as a method of ensuring confidentiality and integrity of data in transit.
		SC-8(1)	**Transmission Confidentiality and Integrity:** Cryptographic Protection	The TOE's use of IPsec provides a cryptographic means to protect data in transit.
		SC-13	**Cryptographic Protection**	The TOE provides cryptographic methods to secure data in transit, which may satisfy organization-defined uses if the functionality claimed by the TSF is consistent with organizational requirements.
FCS_KDF_EXT.1	**Cryptographic Key Derivation**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE has the ability to derive keys in support of the key lifecycle process.
FCS_PCC_EXT.1	**Cryptographic Password Construct and Conditioning**	IA-5(1)	**Authenticator Management:** Password-Based Authentication	A compliant TOE has the ability to condition stored passwords, which satisfies part (c) of this control.
		SC-13	**Cryptographic Protection**	A conformant TOE has the ability to perform password-based key derivation based on FIPS- and NSA-approved standards.
FCS_SMC_EXT.1	**Submask Combining**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE has the ability to perform submask combining in support of key generation functions.
FCS_SNI_EXT.1	**Cryptographic Operation (Salt, Nonce, and Initialization Vector Generation)**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE's use of salts, nonces, and/or IVs as needed ensures that cryptographic keys are generated appropriately.
FCS_SSH_EXT.1	**SSH-Selected**	AC-17(2)	**Remote Access:** Protection of Confidentiality and	The SSH client protocol implemented by the TOE provides confidentiality and integrity for remote access.

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
			Integrity Using Encryption	
		IA-2	**Identification and Authentication (Organizational Users)**	A conformant TOE may use SSH functionality to interact with a remote system on behalf of an organizational user.
		IA-3	**Device Identification and Authentication**	A conformant TOE may use SSH functionality to establish a static or as-needed connection to a specific remote device that is authenticated using a public key or X.509 certificate (instead of an administrator-supplied credential), which supports this control.
		SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE has the ability to ensure the confidentiality and integrity of information transmitted between the TOE and another trusted IT product.
		SC-8(1)	**Transmission Confidentiality and Integrity:** Cryptographic Protection	The TOE's use of SSH supports a cryptographic method of protecting data in transit.
		SC-13	**Cryptographic Protection**	The TOE provides cryptographic methods to secure data in transit, which may satisfy organization-defined uses if the functionality claimed by the TSF is consistent with organizational requirements.
FCS_TLS_EXT.1	**TLS Selected**	SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE has the ability to ensure the confidentiality and integrity of information transmitted between the TOE and another trusted IT product.

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
		SC-8(1)	**Transmission Confidentiality and Integrity:** Cryptographic Protection	The TOE supports a cryptographic method of protecting data in transit.
		SC-13	**Cryptographic Protection**	The TOE provides cryptographic methods to secure data in transit, which may satisfy organization-defined uses if the functionality claimed by the TSF is consistent with organizational requirements.
FIA_PSK_EXT.1	**Pre-Shared Key Composition**	IA-5	**Authenticator Management**	A conformant TOE uses pre-shared keys as a type of authenticator and will ensure their strength and confidentiality, which supports parts (c) and (g) of the control.
Objective Requirements				
This PP has no objective requirements.				