Mapping Between

Standard Protection Profile for Enterprise Security Management, Policy Management, Version 2.1, 2013-10-24

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-3, SC-7(10), PL-9**. The primary purpose of an ESM Policy Management product is to act as a centralized configuration point for one or more ESM Access Control products. It therefore supports AC-3 or SC-7(10) at a high level by defining the access control policy that is enforced, depending on the type of access control product being managed. In general, an ESM Policy Management product will support AC-3; SC-7(10) is only applicable if the capability being managed is for data loss prevention and the ESM Policy Management product is used to configure rules to prevent data from transiting the boundary of a system. The product is also intended to fulfill PL-9 at a high level since the policy is defined at a central point and enforced on all subjects rather than being separately configured at each individual enforcement point. Individual SFRs may relate to other security controls to ensure the secure implementation of the functions that are performed in support of this, but the reader should be aware that those are all implemented in support of ensuring the proper definition of policies that are enforced by other parts of the information system. Since the role of the TOE is to act as the configuration point for ESM Access Control products, many of its security functions relate to the TOE's ability to interact with these (i.e. by transmitting policies or other configuration settings that affect the behavior of the recipient).
- **SA-4(7).** Perhaps it is needless to say, but satisfaction of any NIAP PP or PP-Configuration 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
TOE Security Functional Requirements				
ESM_ACD.1*	**Access Control Policy Definition**	AC-3	**Access Enforcement**	The TOE supports this control through its ability to define access control policies. Although AC-3 focuses on the enforcement of access control policies, critical to enforcement is the ability to define the policy to be enforced. The PP does not mandate a specific type of access control policy be enforced (e.g. mandatory, discretionary, role-based) so any applicable sub-controls will depend on the specific functionality of the TOE.
ESM_ACT.1	**Access Control Policy Transmission**	AC-3	**Access Enforcement**	A conformant TOE will provide a mechanism to update the security configuration of an ESM Access Control product.
		CM-6	**Configuration Settings**	The TOE supports part (b) of this control by providing a mechanism to define and enforce configuration settings for ESM Access Control products.
ESM_EAU.2	**Reliance on Enterprise Authentication**	IA-2 -or- IA-8	**Identification and Authentication (Organizational Users)** **-or-** **Identification and Authentication (Non-Organizational Users)**	A conformant TOE supports this control by implementing or invoking a mechanism to authenticate users so that appropriate access control policies can be enforced. These users may be from inside or outside the organization.
ESM_EID.2	**Reliance on Enterprise Identification**	IA-2 -or- IA-8	**Identification and Authentication (Organizational Users)** **-or-**	A conformant TOE supports this control by implementing or invoking a mechanism to identify users so that appropriate access control policies can be enforced. These users may

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
			Identification and Authentication (Non-Organizational Users)	be from inside or outside the organization.
FAU_GEN.1	**<u>Audit Data Generation</u>**	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 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

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
				control and if the TOE's audit log is part of the overall system's auditing.
FAU_SEL_EXT.1*	**External Selective Audit**	AU-12	**Audit Record Generation**	A conformant TOE supports part (b) of this control by implementing a mechanism to determine the events that cause audit records to be generated.
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	**Protection of Audit Information**	A conformant TOE has the ability to prevent unauthorized modification and deletion of audit records.
		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.
FIA_USB.1	**User-Subject Binding**	AC-3	**Access Enforcement**	A conformant TOE supports this control by implementing a mechanism to associate administrators with their subject identity on the TOE for the purposes of determining the functions that they are authorized to perform.
FMT_MOF.1	**Management of Functions Behavior**	AC-3	**Access Enforcement**	A conformant TOE will not permit configuration of its

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
				functionality unless proper authorization is provided.
		AC-6	**Least Privilege**	A conformant TOE enforces least privilege by restricting the users that are able to manage TOE functionality.
FMT_MOF_EXT.1*	**External Management of Functions Behavior**	AC-3	**Access Enforcement**	A conformant TOE will not permit its use to configure an external ESM Access Control product unless proper authorization is provided.
		AC-6	**Least Privilege**	A conformant TOE enforces least privilege by restricting the users that are able to use the TOE to manage an external ESM Access Control product.
FMT_MSA_EXT.5	**Consistent Security Attributes**	N/A	**N/A**	This SFR requires the TSF to define consistent security attributes for access control policies and take action when inconsistencies are detected. There are no specific controls that require defined attributes to be consistent.
FMT_SMF.1	**Specification of Management Functions**	CM-6	**Configuration Settings**	A conformant TOE may satisfy one or more optional 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 Management Roles**	AC-2(7)	**Account Management:** Privileged User Accounts	A conformant TOE has the ability to associate a Policy Management product acting on behalf of an administrator with a privileged role that allows for its configuration to be changed.

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
FPT_APW_EXT.1	**Protection of Stored Credentials**	AC-3(11)	**Access Enforcement:** Restrict Access to Specific Information Types	A conformant TOE restricts access to administrative credentials, which supports the control to the extent that such a repository is identified by the organization as requiring restricted access.
		IA-5	**Authenticator Management**	A conformant TOE protects authentication data from unauthorized disclosure, in support of part (g) of this control.
FPT_SKP_EXT.1	**Protection of Secret Key Parameters**	AC-3(11)	**Access Enforcement:** Restrict Access to Specific Information Types	A conformant TOE restricts access to the key storage repository, which supports this control if such a repository is identified by the organization as requiring restricted access.
		IA-5	**Authenticator Management**	If the stored key data includes an authenticator (such as an SSH private key), a conformant TOE protects authentication data from unauthorized disclosure, in support of part (g) of this control.
		SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE supports the enforcement of this control by protecting stored cryptographic data. If that cryptographic data includes authentication data, it supports IA-5 part (g) as well.
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.

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.
FTP_TRP.1	**Trusted Path**	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 users and itself.
Optional Requirements				
ESM_ATD.1	**Object Attribute Definition**	AC-3	**Access Enforcement**	A conformant TOE supports this control by defining object attributes that can be used to make access control decisions.
ESM_ATD.2	**Subject Attribute Definition**	AC-3	**Access Enforcement**	A conformant TOE supports this control by defining subject attributes that can be used to make access control decisions.
FAU_SEL.1	**Selective Audit**	AU-12	**Audit Record Generation**	A conformant TOE supports part (b) of this control by implementing a mechanism to determine the events that cause audit records to be generated.
FCS_CKM.1	**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 Management:** Asymmetric Keys	A conformant TOE ensures that generated asymmetric keys provide an appropriate level of security.

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
FCS_CKM_EXT.4	**Cryptographic Key Zeroization**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE has the ability to securely destroy cryptographic keys.
FCS_COP.1(1)	**Cryptographic Operation (for Data Encryption/Decryption)**	SC-13	**Cryptographic Protection**	A conformant TOE has the ability to perform symmetric encryption and decryption using NSA-approved and FIPS-validated algorithms.
FCS_COP.1(2)	**Cryptographic Operation (for Cryptographic Signature)**	SC-13	**Cryptographic Protection**	A conformant TOE has the ability to perform cryptographic signing using NSA-approved and FIPS-validated algorithms.
FCS_COP.1(3)	**Cryptographic Operation (for Cryptographic Hashing)**	SC-13	**Cryptographic Protection**	A conformant TOE has the ability to perform cryptographic hashing using NSA-approved and FIPS-validated algorithms.
FCS_COP.1(4)	**Cryptographic Operation (for Cryptographic 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_HTTPS_EXT.1	**HTTPS**	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

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
				organizational requirements.
FCS_IPSEC_EXT.1	**IPsec**	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.
		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_RBG_EXT.1	**Cryptographic Operation (Random Bit Generation)**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE's use of an appropriate DRBG ensures that generated keys provide an appropriate level of security.
FCS_SSH_EXT.1	**SSH**	AC-17(2)	**Remote Access:** Protection of Confidentiality and Integrity Using Encryption	The SSH client protocol implemented by the TOE provides confidentiality and integrity for remote access.
		IA-2	**Identification and Authentication (Organizational Users)**	A conformant TOE may use its SSH client functionality to interact with a remote system on behalf of an organizational user.
		IA-3	**Device Identification and Authentication**	A conformant TOE may use its SSH client functionality to establish a static or as-needed connection to a specific remote device that is authenticated using a

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
				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**	IA-5(2)	**Authenticator Management:** Public Key-Based Authentication	The TOE requires peers to possess a valid certificate before establishing trusted communications, supporting 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 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.

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
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_SOS.1	**Verification of Secrets**	IA-5(1)	**Authenticator Management:** Password-Based Authentication	A conformant TOE will have the ability to enforce some minimum password complexity requirements, although they are not identical to CNSS or DoD requirements or to those specified in part (a) of this control.
FMT_MTD.1	**Management of TSF Data**	AC-3	**Access Enforcement**	A conformant TOE supports this control by defining object attributes that can be used to make access control decisions.
		AC-3(7)	**Access Enforcement:** Role-Based Access Control	A conformant TOE supports this control by having the ability to limit the functions that can be performed based on role.
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.
FTA_SSL_EXT.1	**TSF-Initiated Session Locking**	AC-11	**Device Lock**	A conformant TOE may have the ability to lock an idle local interactive session, depending on the selection made in the SFR.
		AC-12	**Session Termination**	A conformant TOE may have the ability to terminate an idle local interactive session, depending on the selection made in the SFR.
		IA-11	**Re-Authentication**	A conformant TOE may have the ability to require user re-authentication after the termination an idle local interactive session, depending on the selection made in the SFR.

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
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 idle remote interactive session.
FTA_SSL.4	**User-Initiated Termination**	AC-12(1)	**Session Termination:** User-Initiated Logouts	A conformant TOE has the ability to terminate an active session upon user request.
FTA_TSE.1	**TOE Session Establishment**	AC-2(11)	**Account Management:** Usage Conditions	A conformant TOE supports this control by enforcing usage conditions that prevent otherwise valid subjects from accessing objects that are protected by the TSF.
Selection-Based Requirements				
FTA_TAB.1	**TOE Access Banner**	AC-8	**System Use Notification**	A conformant TOE displays an advisory warning to the user prior to authentication.
		AC-14	**Permitted Actions Without Identification or Authentication**	A conformant TOE displays an advisory warning to the user prior to authentication.
		PL-4	**Rules of Behavior**	The TOE displays an advisory warning to the user prior to authentication to identify the rules that describe their responsibilities and expected behavior for information and system usage, security, and privacy.
Objective Requirements				
No objective requirements defined.				