Mapping Between
Protection Profile for Certification Authorities,
Version 2.1, 1-December-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.
- **IA-4, IA-5(2), and SC-17.** The primary purpose of a Certification Authority (CA) product is to handle the distribution and maintenance of identifiers, specifically in support of a PKI infrastructure. Therefore, a conformant TOE as a whole supports system satisfaction of IA-4, IA-5(2), and SC-17 at a general level. 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 SC-17 is the behavior that a CA is intended to address.
- **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.
- **TOE vs OE implementation.** Many SFRs in this PP describe functionality that may be implemented either by the TOE itself or through TSF implication of a similarly-validated component in its operational environment (i.e., a general-purpose operating system). Those SFRs that may be implemented in this manner are denoted with an asterisk (*).

Common Criteria Version 3.x SFR		Supports Enforcement of NIST SP 800-53 Revision 5 Control		Comments and Observations
FAU_ADP_EXT.1*	**Audit Dependencies**	AU-2	**Event Logging**	A conformant TOE has the ability to generate audit records for various events. It may also make use of the operational environment to generate a subset of the required audit records.
FAU_GCR_EXT.1*	**Generation of Certificate Repository**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE partially supports the enforcement of this control by storing certificates and potentially CRLs using either TSF or environmental mechanisms.
FAU_GEN.1*	**Audit Data Generation**	AU-2	**Event Logging**	A conformant TOE has the ability to generate audit records for various events. It may also make use of the operational environment to generate a subset of the required audit records. 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. It may also make use of the operational environment to satisfy this control.
		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. It may also make use of the operational environment to satisfy this control.
		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). It may also make use of the operational environment to satisfy this control.
FAU_GEN.2*	**User Identity Association**	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.
FAU_STG.4	**Prevention of Audit Data Loss**	AU-4	**Audit Log Storage Capacity**	A conformant TOE supports the enforcement of this control by allocating storage for audit data.

		AU-5	**Response to Audit Logging Process Failures**	A conformant TOE supports the enforcement of part (b) of this control by taking some action in the event that audit data cannot be written. This SFR does not require an alerting method (e.g. as defined by FAU_ARP.1) so part (a) is not applicable.
FCO_NRO_EXT.2	**Certificate-Based Proof of Origin**	AU-10	**Non-repudiation**	A conformant TOE enforces non-repudiation through verification of certificate origin.
		AU-10(1)	**Non-repudiation** Association of Identities	A conformant TOE supports the enforcement of part (a) of this control through its binding of its issued certificates. It supports the enforcement of part (b) of this control by associating its own identity with its issued certificates.
		AU-10(2)	**Non-repudiation** Validate Binding of Information Producer Identity	A conformant TOE may support this control by having a mechanism for verifying proof of origin for revocation requests.
FCS_CDP_EXT.1*	**Cryptographic Dependencies**	SC-12 or SC-13	**Cryptographic Key Establishment and Management** **-or-** **Cryptographic Protection**	Depending on the selections made in this SFR, a conformant TOE or its operational environment supports the enforcement of one or both of these controls. Specific control applicability for each selection can be found in the mappings for the individual SFRs that the selection items represent.
FCS_STG_EXT.1*	**Cryptographic Key Storage**	IA-5	**Authenticator Management**	A conformant TOE protects private key data used as authenticators from unauthorized disclosure, either through its own mechanisms or through environmental ones, in support of part (h) of this control.
		SC-12	**Cryptographic Key**	A conformant TOE supports the enforcement

			Establishment and Management	of this control by protecting stored cryptographic data, either through its own mechanisms or through invocation of environmental ones.
FDP_CER_EXT.1	**Certificate Profiles**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE partially supports the enforcement of this control by defining parameters for certificate generation.
		SC-17	**Public Key Infrastructure Certificates**	A conformant TOE implements a certificate profile function and ensures that certificates are generated following the policy defined by that function.
FDP_CER_EXT.2	**Certificate Request Matching**	AU-10	**Non-repudiation**	A conformant TOE supports the implementation of this control through association of certificates and the entities that request them.
FDP_CER_EXT.3	**Certificate Issuance Approval**	SC-17	**Public Key Infrastructure Certificates**	A conformant TOE implements a certificate profile function and ensures that certificates are approved in accordance with the policy defined by that function.
		SC-23(5)	**Session Authenticity:** Allowed Certificate Authorities	A conformant TOE supports the enforcement of this control by allowing the TSF to act as an allowed CA for approving certificates.
FDP_CSI_EXT.1	**Certificate Status Information**	IA-5(2)	**Authenticator Management:** Public Key-Based Authentication	A conformant TOE supports part (b) of this control through a mechanism that allows external entities to determine whether the presented certificate is valid.
		SC-17	**Public Key Infrastructure Certificates**	A conformant TOE supports the issuance of PKI certificates by generating status information about the certificates it has issued.

FDP_RIP.1*	**Subset Residual Information Protection**	SC-4	**Information in Shared System Resources**	A conformant TOE ensures, either through its own mechanisms or through invocation of its operational environment, that residual data stored in data buffers is purged prior to re-use of those buffers.
		SC-8(2)	**Transmission Confidentiality and Integrity:** Pre- and Post-Transmission Handling	A conformant TOE and potentially the operational environment ensures that any previous information content of certificate authority functions and network communications is made unavailable before reuse.
FIA_X509_EXT.1*	**Certificate Validation**	IA-5(2)	**Authenticator Management:** Public Key-Based Authentication	A conformant TOE has the ability to validate certificate path and status or invoke an environmental service to do this, which satisfies this control.
		SC-23	**Session Authenticity**	Depending on the TOE's use of trusted communications channels, it may use X.509 certificate validation in support of session authentication.
		SC-23(5)	**Session Authenticity:** Allowed Certificate Authorities	If the TOE uses X.509 certificates as part of session authentication, it will include the functionality needed to validate certificate authorities or invoke this functionality in its operational environment.
FIA_X509_EXT.2*	**Certificate-Based Authentication**	CM-14	**Signed Components**	A conformant TOE supports the enforcement of this control by using code signing certificates for software updates or invokes this functionality in its operational environment.
		IA-2	**Identification and Authentication (Organizational Users)**	A conformant TOE has the ability to identify and authenticate organizational users via X.509 certificates.

		SI-7(15)	**Software, Firmware, and Information Integrity:** Code Authentication	A conformant TOE's use of a code signing certificate for software updates supports the enforcement of this control. It may make use of the operational environment to support the enforcement of this control.
FIA_UAU_EXT.1*	**Authentication Mechanism**	IA-2	**Identification and Authentication (Organizational Users)**	A conformant TOE has the ability to provide an authentication mechanism for privileged users, or to interface with its operational environment to provide this.
FIA_UIA_EXT.1	**User Identification and 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	**Identification and Authentication (Organizational Users)**	A conformant TOE has the ability to require that certain functions require successful authentication to access, whether provided by the TOE itself or its environment.
FMT_MOF.1(1)*	**Management of Security Functions Behavior (Administrator Functions)**	AC-3(7)	**Access Enforcement:** Role-Based Access Control	A conformant TOE supports the enforcement of this control by specifying the management functions that are available to the Administrator role as opposed to other defined roles.
		AC-6	**Least Privilege**	A conformant TOE or the operational environment enforces least privilege by defining the minimum set of relevant management functions that are available to the Administrator role as opposed to other defined roles.
		AC-6(1)	**Least Privilege:** Authorize Access to Security Functions	A conformant TOE or the operational environment defines its management authorizations such that explicit authorization is required to perform a management function.

FMT_MOF.1(2)*	**Management of Security Functions Behavior (CA/RA Functions)**	AC-3(7)	**Access Enforcement:** Role-Based Access Control	A conformant TOE or the operational environment supports the enforcement of this control by specifying the management functions that are available to the CA Operations Staff or RA Staff role as opposed to other defined roles.
		AC-6	**Least Privilege**	A conformant TOE or the operational environment enforces least privilege by defining the minimum set of relevant management functions that are available to the CA Operations Staff or RA Staff role as opposed to other defined roles.
		AC-6(1)	**Least Privilege:** Authorize Access to Security Functions	A conformant TOE or the operational environment defines its management authorizations such that explicit authorization is required to perform a management function.
FMT_MOF.1(3)*	**Management of Security Functions Behavior (CA Operations Functions)**	AC-3(7)	**Access Enforcement:** Role-Based Access Control	A conformant TOE or the operational environment supports the enforcement of this control by specifying the management functions that are available to the CA Operations Staff role as opposed to other defined roles.
		AC-6	**Least Privilege**	A conformant TOE or the operational environment enforces least privilege by defining the minimum set of relevant management functions that are available to the CA Operations Staff role as opposed to other defined roles.
		AC-6(1)	**Least Privilege:** Authorize Access to Security Functions	A conformant TOE or the operational environment defines its management authorizations such that explicit authorization is required to perform a management function.

FMT_MOF.1(4)*	**Management of Security Functions Behavior (Admin/Officer Functions)**	AC-3(7)	**Access Enforcement:** Role-Based Access Control	A conformant TOE or the operational environment supports the enforcement of this control by specifying the management functions that are available to the Administrator, Auditor, or CA Operations Staff role as opposed to other defined roles.
		AC-6	**Least Privilege**	A conformant TOE or the operational environment enforces least privilege by defining the minimum set of relevant management functions that are available to the Administrator, Auditor, or CA Operations Staff role as opposed to other defined roles.
		AC-6(1)	**Least Privilege:** Authorize Access to Security Functions	A conformant TOE or the operational environment defines its management authorizations such that explicit authorization is required to perform a management function.
FMT_MOF.1(5)*	**Management of Security Functions Behavior (Auditor Functions)**	AC-3(7)	**Access Enforcement:** Role-Based Access Control	A conformant TOE or the operational environment supports the enforcement of this control by specifying the management functions that are available to the Auditor role as opposed to other defined roles.
		AC-6	**Least Privilege**	A conformant TOE or the operational environment enforces least privilege by defining the minimum set of relevant management functions that are available to the Auditor role as opposed to other defined roles.
		AC-6(1)	**Least Privilege:** Authorize Access to Security Functions	A conformant TOE or the operational environment defines its management authorizations such that explicit authorization is required to perform a management function.

FMT_MTD.1	**Management of TSF Data**	AC-3(7)	**Access Enforcement:** Role-Based Access Control	A conformant TOE supports this control by restricting the management of TSF data to privileged users.
		AC-6	**Least Privilege**	A conformant TOE supports this control by restricting the management of TSF data to privileged users.
		AC-6(1)	**Least Privilege:** Authorize Access to Security Functions	A conformant TOE supports this control by restricting the management of TSF data to privileged users.
FMT_SMF.1*	**Specification of Management Functions**	CM-6	**Configuration Settings**	A conformant TOE or the operational environment 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.2*	**Restrictions on Security Roles**	AC-2(7)	**Account Management:** Privileged User Accounts	A conformant TOE and potentially its operational environment maintains roles and is able to associate users with roles, in support of part (a) of the control.
		AC-5	**Separation of Duties**	A conformant TOE or potentially its operational environment enforces separation of duties of individuals and roles
FPT_FLS.1	**Failure with Preservation of Secure State**	SC-24	**Fail in Known State**	A conformant TOE preserves a secure state in the event of a failure.
FPT_KST_EXT.1*	**No Plaintext Key Export**	MP-5	**Media Transport**	A conformant TOE and optionally the operational environment prevents the export of plaintext keys, including to any physical media attached to the

				system on which the TOE is running.
		SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE supports the enforcement of this control by ensuring that key data exported from the TOE is protected. It may also make use of the operational environment to provide this functionality
		SC-8(1)	**Transmission Confidentiality and Integrity:** Cryptographic Protection	A conformant TOE supports the enforcement of this control by ensuring that key data exported from the TOE is encrypted. It may also make use of the operational environment to provide this functionality.
		SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE supports the enforcement of this control by ensuring the protection of stored cryptographic data. It may also make use of the operational environment to provide this functionality.
FPT_KST_EXT.2*	**TSF Key Protection**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE supports the enforcement of this control by ensuring the protection of stored cryptographic data. It may also make use of the operational environment to provide this functionality.
FPT_RCV.1	**Manual Trusted Recovery**	CP-10	**System Recovery and Reconstitution**	A conformant TOE supports the enforcement of this control by providing a mechanism for itself to be restored to a secure state following a failure.
		CP-12	**Safe Mode**	A conformant TOE supports the enforcement of this control through its support of a maintenance mode, which is equivalent to the 'safe mode' specified by this control.
FPT_SKP_EXT.1*	**Protection of Keys**	AC-3(11)	**Access Enforcement:**	A conformant TOE restricts access to the key storage

			Restrict Access to Specific Information Types	repository, which supports this control if such a repository is identified by the organization as requiring restricted access.
		SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE supports the enforcement of this control by protecting stored cryptographic data, either through the TSF or through reliance on the operational environment.
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_TUD_EXT.1*	**Trusted Update**	CM-14	**Signed Components**	A conformant TOE requires that updates to it include digital signatures for integrity measures, either through the TSF or through reliance on the operational environment.
		SI-7(1)	**Software, Firmware, and Information Integrity:** Integrity Checks	A conformant TOE has the ability to verify the integrity of updates to it, either through the TSF or through reliance on the operational environment.
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, either through the TSF or through reliance on the operational environment.
FTA_TAB.1	**Default TOE Access Banners**	AC-8	**System Use Notification**	A conformant TOE displays an advisory warning to the user prior to authentication.
FTP_TRP.1	**Trusted Path**	IA-3(1)	**Device Identification and Authentication:** Cryptographic	A conformant TOE may support the enforcement of this control if the protocol(s) used to establish trusted

			Bidirectional Authentication	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				
FCS_COP.1(5)*	**Cryptographic Operation (Password-Based Key Derivation Function)**	SC-13	**Cryptographic Protection**	A conformant TOE has the ability to perform or invoke environmental services for key derivation using NSA-approved and FIPS-validated algorithms.
FDP_CER_EXT.4	**Non-X.509v3 Certificate Generation**	SC-17	**Public Key Infrastructure Certificates**	A conformant TOE implements a certificate profile function and ensures that X.509 certificates in formats other than v3 are generated following the policy defined by that function.
FDP_SDP_EXT.1*	**User Sensitive Data Protection**	SC-28	**Protection of Information at Rest**	A conformant TOE or the operational environment has the ability to protect sensitive information at rest. This supports the enforcement of the control through use by the Privacy Overlay to protect PII.
FDP_STG_EXT.1	**Public Key Protection**	AC-3 or SI-7	**Access Enforcement** **-or-** **Software, Firmware, and Information Integrity**	A conformant TOE will use access control or integrity protection to protect key and certificate data.
		IA-5	**Authenticator Management**	A conformant TOE supports part (h) of this control by ensuring the confidentiality or integrity of stored public key and certificate data.

FPT_NPE_EXT.1	**NPE Constraints**	SC-17	**Public Key Infrastructure Certificates**	A conformant TOE enforces a certificate issuance policy through an administrator-configurable ruleset that specifies authorizations to submit non-person entity certificate requests.
FPT_SKY_EXT.1*	**Split Knowledge Procedures**	AC-3(2)	**Access Enforcement:** Dual Authorization	A conformant TOE supports the enforcement of this control by requiring split knowledge procedures for export of key data, either through its own functionality or by interfacing with its operational environment.
		CP-9	**System Backup**	A conformant TOE supports the enforcement of part (b) of this control because the key data being exported from the TOE is system-level information that is being stored externally in the case that a recovery from failure is needed (i.e., the key data is backed up). Part (d) is enforced through the use of split knowledge procedures that ensure the confidentiality of this data is maintained while outside the TOE boundary. Note that this only applies to backup of the system-level data stored by the TOE and is not necessarily integrated with an organization-wide backup solution.
FPT_TST_EXT.1*	**TOE Integrity Test**	SI-6	**Security and Privacy Function Verification**	A conformant TOE or the operational environment will run automatic tests to ensure correct operation of its own functionality.
		SI-7	**Software, Firmware, and Information Integrity**	A conformant TOE or the operational environment supports the enforcement of this control by including an integrity checking mechanism for itself.

		SI-7(1)	**Software, Firmware, and Information Integrity:** Integrity Checks	A conformant TOE or the operational environment supports the enforcement of this control by including an integrity checking mechanism for itself.
		SI-7(12)	**Software, Firmware, and Information Integrity**: Integrity Verification	A conformant TOE or the operational environment supports the enforcement of this control by providing an integrity verification mechanism for the TOE software.
FPT_TST_EXT.2	**Integrity Test**	SI-7	**Software, Firmware, and Information Integrity**	A conformant TOE supports the enforcement of this control by including an integrity checking mechanism for its stored data.
		SI-7(1)	**Software, Firmware, and Information Integrity:** Integrity Checks	A conformant TOE supports the enforcement of this control by including an integrity checking mechanism for its stored data.
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_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.
Selection-Based Requirements				

FCS_CKM_EXT.1(1)*	**Symmetric Key Generation for DEKs**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE supports the enforcement of this control by using a mechanism to generate DEKs, either through the TSF or through reliance on the operational environment.
		SC-12(2)	**Cryptographic Key Establishment and Management:** Symmetric Keys	The TOE generates or interfaces with the operational environment to generate DEKs, which are symmetric keys.
FAU_SCR_EXT.1*	**Certificate Repository Review**	N/A	**N/A**	N/A – this function allows searches to be performed for certificate data based on specified fields. It does not relate to the enforcement of any security controls.
FAU_SAR.1	**Audit Review**	AU-6(7)	**Audit Record Review, Analysis, and Reporting:** Permitted Actions	A conformant TOE supports the enforcement of this control by limiting access to the audit review function to members of the Auditor role.
		AU-7	**Audit Reduction and Report Generation**	A conformant TOE supports the enforcement of this control by providing a mechanism to read audit information.
FAU_SAR.3	**Selectable Audit Review**	AU-7	**Audit Reduction and Report Generation**	A conformant TOE supports the enforcement of this control by providing a mechanism to review stored audit data.
		AU-7(1)	**Audit Reduction and Report Generation:** Automatic Processing	A conformant TOE supports the enforcement of this control by allowing for the definition of audit search criteria that can be used to search for and read an auditor-defined subset of the audit records.
FAU_SEL.1	**Selective Audit**	AU-12	**Audit Record Generation**	A conformant TOE supports part (b) of this control by allowing authorized users to specify the auditable events that the TSF will generate.

FAU_STG.1(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.1(2)	**Protected Audit Trail Storage (Archive Data)**	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.
		AU-11	**Audit Record Retention**	A conformant TOE supports the enforcement of this control by defining 'archive' audit records that can have extended retention requirements in accordance with organizational procedures.
FAU_STG_EXT.1	**External Audit Trail Storage**	AU-4	**Audit Log Storage Capacity**	A conformant TOE shall maintain availability and integrity of audit data by storing it locally on the TOE or TOE platform, or on an external IT entity using a trusted channel protocol.
		AU-4(1)	**Audit Log Storage Capacity:** Transfer	A conformant TOE has the ability to transmit audit

			to Alternate Storage	data to a location in its operational environment using a trusted channel protocol.
		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 has the ability to transmit audit data to a location in its operational environment using a trusted channel protocol.
FAU_STG_EXT.2	**Audit Data Retention**	AU-11	**Audit Record Retention**	A conformant TOE supports the enforcement of this control by defining 'archive' audit records that can have extended retention requirements in accordance with organizational procedures.
FCS_CKM.1*	**Cryptographic Key Generation**	SC-12	**Cryptographic Key Establishment and Management**	The ability of the TOE to generate asymmetric keys or invoke interfaces provided by the operational environment 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 or the invoking interfaces provided by the operational environment to generated asymmetric keys provide an appropriate level of security.
FCS_CKM.2*	**Cryptographic Key Establishment**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE or interfaces provided by the operational environment supports this control by providing a key establishment function.
		SC-12(3)	**Cryptographic Key Establishment and Management:** Asymmetric Keys	A conformant TOE or interfaces provided by the operational environment supports the production of

				asymmetric keys by providing a key establishment function.
FCS_CKM_EXT.1(3)*	**Key Generation for Key Encryption Keys (TOE Key Archival)**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE supports the key generation portion of this control by generating, or interfacing with its operational environment to generate, key encryption keys. The TOE will also support SC-12(2) or SC-12(3), depending on whether it uses symmetric or asymmetric keys for this purpose.
FCS_CKM_EXT.1(4)*	**Generation of Key Shares**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE supports the key generation portion of this control by generating, or interfacing with its operational environment to generate, key shares. The TOE will also support SC-12(2) or SC-12(3), depending on whether it uses symmetric or asymmetric keys for this purpose.
FCS_CKM_EXT.4*	**Cryptographic Key Destruction**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE securely destroys or interfaces with the operational environment to securely destroy cryptographic keys.
FCS_CKM_EXT.5*	**Public Key Integrity**	SI-7(6)	**Software, Firmware, and Information Integrity:** Cryptographic Protection	A conformant TOE supports the enforcement of this control by using cryptographic methods to protect the integrity of stored key data either through the TSF or through reliance on the operational environment.
FCS_CKM_EXT.6*	**TOE Key Archival**	CP-10	**System Recovery and Reconstitution**	A conformant TOE supports the enforcement of this control by providing a mechanism, either internal to the TOE or invoked from its operational environment, to import/export a key

				archive to maintain continuity of operations in the event of a TSF failure.
		SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE supports the enforcement of this control by protecting the stored key archive, either within the TSF or through invocation of an environmental interface.
FCS_COP.1(1)*	**Cryptographic Operation (AES Encryption/ Decryption)**	SC-13	**Cryptographic Protection**	A conformant TOE performs or interfaces with the operational environment to perform symmetric encryption and decryption using NSA-approved and FIPS-validated algorithms.
FCS_COP.1(2)*	**Cryptographic Operation (Cryptographic Signature)**	SC-13	**Cryptographic Protection**	A conformant TOE performs or interfaces with the operational environment to perform cryptographic signing using NSA-approved and FIPS-validated algorithms.
FCS_COP.1(3)*	**Cryptographic Operation (Cryptographic Hashing)**	SC-13	**Cryptographic Protection**	A conformant TOE performs or interfaces with the operational environment to perform cryptographic hashing using NSA-approved and FIPS-validated algorithms.
FCS_COP.1(4)*	**Cryptographic Operation (Keyed-Hash Message Authentication)**	SC-13	**Cryptographic Protection**	A conformant TOE performs or interfaces with the operational environment to perform keyed-hash message authentication using NSA-approved and FIPS-validated algorithms.
FCS_RBG_EXT.1*	**Cryptographic 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 either through the TSF or through reliance on the operational environment.
FIA_AFL.1*	**Authentication Failure Handling**	AC-7	**Unsuccessful Logon Attempts**	The TOE or through reliance on the operational environment has the

				ability to detect when a defined number of unsuccessful authentication attempts occur and take some corrective action.
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, although they are not identical to CNSS or DoD requirements or to those specified in part (a) of this control.
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.
FPT_APW_EXT.1	**Protection of Privileged User Passwords**	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 (h) of this control.
		IA-5(6)	**Authenticator Management:** Protection of Authenticators	A conformant TOE must have the ability to securely store passwords and other credential data it uses.
		SC-28(1)	**Protection of Information at Rest:** Cryptographic Protection	A conformant TOE uses a cryptographic mechanism to prevent credential data at rest from being stored in plaintext.
FCO_NRR_EXT.2	**Certificate-Based Proof of Receipt**	AU-10	**Non-repudiation**	A conformant TOE supports enforcement of this control by providing proof of receipt for CMC or EST data.
		AU-10(1)	**Non-repudiation:** Association of Identities	A conformant TOE binds its identity to proof of receipt using digital signature.

FIA_CMCS_EXT.1	**Certificate Management over CMS (CMC) Server**	SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE uses HTTPS to protect CMC data in transit.
		SC-8 (1)	**Transmission Confidentiality and Integrity:** Cryptographic Protection	A conformant TOE uses HTTPS to protect CMC data in transit.
		SC-17	**Public Key Infrastructure Certificates**	A conformant TOE acts as a CMC server as part of the certificate issuance process.
FIA_CMCC_EXT.1	**Certificate Management over CMS (CMC) Client**	SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE uses HTTPS to protect CMC data in transit.
		SC-8(1)	**Transmission Confidentiality and Integrity:** Cryptographic Protection	A conformant TOE uses HTTPS to protect CMC data in transit.
		SC-17	**Public Key Infrastructure Certificates**	A conformant TOE acts as a CMC client as part of the certificate issuance process.
FIA_ESTS_EXT.1	**Enrollment over Secure Transport (EST) Server**	SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE uses TLS to protect EST data in transit.
		SC-8(1)	**Transmission Confidentiality and Integrity:** Cryptographic Protection	A conformant TOE uses TLS to protect EST data in transit.
		SC-17	**Public Key Infrastructure Certificates**	A conformant TOE acts as an EST server as part of the certificate issuance process.
FIA_ESTC_EXT.1	**Enrollment over Secure Transport (EST) Client**	SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE uses TLS to protect EST data in transit.
		SC-8(1)	**Transmission Confidentiality and Integrity:** Cryptographic Protection	A conformant TOE uses TLS to protect EST data in transit.
		SC-17	**Public Key Infrastructure Certificates**	A conformant TOE acts as an EST client as part of the certificate issuance process.
FIA_X509_EXT.3	**X509 Certificate Request**	SC-17	**Public Key Infrastructure Certificates**	This function supports behavior related to certificate issuance.

FDP_CRL_EXT.1	**Certificate Revocation List Validation**	IA-5(2)	**Authenticator Management:** Public Key-Based Authentication	A conformant TOE supports enforcement of part (a) of this control by serving as a mechanism where certificate status information can be authoritatively checked.
FDP_OCSPG_EXT.1	**OCSP Basic Response Generation**	IA-5(2)	**Authenticator Management:** Public Key-Based Authentication	A conformant TOE supports enforcement of part (a) of this control by serving as a mechanism where certificate status information can be authoritatively checked.
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 any protocols used to establish trusted communications use 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.
FCS_HTTPS_EXT.1	**HTTPS Protocol**	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 Protocol**	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_TLSC_EXT.1	**TLS Client Protocol**	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.
FCS_TLSS_EXT.1	**TLS Server Protocol**	IA-5(2)	**Authenticator Management:** Public Key-Based Authentication	The TOE provides a server certificate to a TLS client 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.
FDP_ITT.1	**Basic Internal Transfer Protection**	SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE will support this control by providing a protected communication channel between remote distributed TOE components.
		SC-8(1)	**Transmission Confidentiality and Integrity**: Cryptographic Protection	A conformant TOE will use cryptographic methods to protect data in transit between different parts of the TOE.
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 (h) of this control.

FPT_ITT.1	**Basic Internal TSF Data Transfer Protection**	SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE will support this control by providing a protected communication channel between remote distributed TOE components.
		SC-8(1)	**Transmission Confidentiality and Integrity**: Cryptographic Protection	A conformant TOE will use cryptographic methods to protect data in transit between different parts of the TOE.
FCS_CKM_EXT.1(2)*	**Key Generation Key Encryption Keys**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE supports the key generation portion of this control by generating, or interfacing with its operational environment to generate, key encryption keys. The TOE will also support SC-12(2) or SC-12(3), depending on whether it uses symmetric or asymmetric keys for this purpose.
FCS_CKM_EXT.7*	**Key Generation for KEKs**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE supports the key generation portion of this control by generating, or interfacing with its operational environment to generate, a root encryption key. The TOE will also support SC-12(2) or SC-12(3), depending on whether it uses symmetric or asymmetric keys for this purpose.
FCS_CKM_EXT.8	**Key Hierarchy Entropy**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE will use a key hierarchy to ensure the secure storage of cryptographic keys.
FPT_SKY_EXT.2*	**Key Share Access**	AC-3	**Access Enforcement**	A conformant TOE supports the enforcement of this control by limiting key share access to individual authorized users.
		AC-5	**Separation of Duties**	A conformant TOE supports the enforcement of this control by ensuring that each key share is only

				accessible by a single privileged user.
Objective Requirements				
FCS_KSH_EXT.1*	**Key Sharing**	AC-3(2)	**Access Enforcement:** Dual Authorization	A conformant TOE supports the enforcement of this control by requiring dual authorization for the export of key data that is used for recovery from TSF failure.
		CP-9	**System Backup**	A conformant TOE supports the enforcement of part (b) of this control because the key data being exported from the TOE is system-level information that is being stored externally in the case that a recovery from failure is needed (i.e., the key data is backed up). Part (d) is enforced through the use of split knowledge procedures that ensure the confidentiality of this data is maintained while outside the TOE boundary. Note that this only applies to backup of the system-level data stored by the TOE and is not necessarily integrated with an organization-wide backup solution.
FIA_ESTC_EXT.2	**EST Client use of TLS-unique value**	SC-17	**Public Key Infrastructure Certificates**	This function supports behavior related to certificate issuance.
FIA_ESTS_EXT.2	**Enrollment over Secure Transport (EST) Server**	SC-17	**Public Key Infrastructure Certificates**	This function supports behavior related to certificate issuance.
FIA_ENR_EXT.1.1	**Certificate Enrollment**	SC-17	**Public Key Infrastructure Certificates**	This function supports behavior related to certificate issuance.