Mapping Between

Protection Profile for Virtualization, Version 1.1, 2021-06-14

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.
- **CP-10, SC-29(1).** One purpose of a virtualization system is to use virtual machines in support of system recovery, which supports CP-10 at a high level. Virtualization technology may also be used to support the deployment of a diversity of operating systems and applications, which supports SC-29(1). However, the use of a virtualization system only supports the ability to enforce these controls based on how it is used; it does not inherently implement these methods on their own.
- **General security purpose for virtualization**. Another purpose of a virtualization system is to minimize system resources by allowing multiple systems to share the same underlying physical platform host. This function is therefore not necessarily security-related, though the use of virtualization can allow organizations to meet certain security controls depending on how the system is used. These include AC-6(4), AC-20(3), CM-7(6), CM-7(7), SC-2, SC-18(5), SC-29(1), SC-30, SC-35, and SI-14. These controls are not enforced by any of the SFR-related behavior specified in the PP; instead, these are the security functions that may be enabled by the use of virtualization technologies. The security functionality of the PP ensures at a general level that the virtualization system can be used to support any of these controls.
- **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				
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 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

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
				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_SAR.1	**Audit Review**	AU-7	**Audit Record Reduction and Report Generation**	A conformant TOE implements an audit report generation functionality.
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.
FAU_STG_EXT.1	**Off-Loading of Audit Data**	AU-4	**Audit Log Storage Capacity**	A conformant TOE allocates some amount of local storage for audit data. It can be used to support the enforcement of this control if the amount of storage is consistent with the assignment chosen for the control.
		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-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. Depending on the actions taken by the TOE when this occurs and on the assignments chosen for this control, the TOE can be used to support the

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
				enforcement of either or both parts of the control.
		AU-5(2)	**Response to Audit Logging Process Failures:** Real-Time Alerts	A conformant TOE has the ability to react in a specific manner when the allocated audit storage space is full. A conformant TOE may support the enforcement of this control, depending on the behavior specified in the ST and the assignments chosen for this control.
		AU-5(4)	**Response to Audit Logging Process Failures:** Shutdown on Failure	A conformant TOE has the ability to react in a specific manner when the allocated audit storage space is full. A conformant TOE may support the enforcement of this control, depending on the behavior specified in the ST and the assignments chosen for this control.
		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.
FCS_CKM.1	**Cryptographic Key Generation**	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.
FCS_CKM.2	**Cryptographic Key Distribution**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE supports this control by providing a key establishment function.
		SC-12(3)	**Cryptographic Key Establishment and**	A conformant TOE supports the production of asymmetric keys by

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
			Management: Asymmetric Keys	providing a key establishment function.
FCS_CKM_EXT.4	**Cryptographic Key Destruction**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE has the ability to securely destroy cryptographic keys.
FCS_COP.1/Hash	**Cryptographic Operation (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/KeyedHash	**Cryptographic Operation (Keyed Hash Algorithms)**	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/Sig	**Cryptographic Operation (Signature Algorithms)**	SC-13	**Cryptographic Protection**	A conformant TOE has the ability to perform cryptographic signing using NSA-approved and FIPS-validated algorithms.
FCS_COP.1/UDE	**Cryptographic Operation (AES 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_ENT_EXT.1	**Entropy for Virtual Machines**	SC-13	**Cryptographic Protection**	A conformant TOE supports this control by providing a mechanism that allows for cryptographic functions that require random number generation to be implemented securely across multiple Guest VMs.
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.
FDP_HBI_EXT.1	**Hardware-Based Isolation Mechanisms**	SC-3(1)	**Security Function Isolation:** Hardware Separation	A conformant TOE makes use of platform hardware mechanisms that ensure that separate Guest VMs accessing the same hardware will remain isolated from one another.
FDP_PPR_EXT.1	**Physical Platform Resource Controls**	SC-6	**Resource Availability**	A conformant TOE supports this control by protecting the availability of physical

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
				platform resources through enforcing Guest VM limitations on their use.
FDP_RIP_EXT.1	**Residual Information in Memory**	SC-4	**Information in Shared System Resources**	A conformant TOE supports this control by clearing residual data from memory so that it is not inadvertently accessible to an unauthorized subject.
FDP_RIP_EXT.2	**Residual Information on Disk**	SC-4	**Information in Shared System Resources**	A conformant TOE supports this control by clearing residual data from disk storage so that it is not inadvertently accessible to an unauthorized subject.
FDP_VMS_EXT.1	**VM Separation**	SC-39	**Process Isolation**	A conformant TOE enforces isolation between Guest VMs except through explicitly-defined mechanisms.
FDP_VNC_EXT.1	**Virtual Networking Components**	AC-4	**Information Flow Enforcement**	A conformant TOE supports this control by implementing a mechanism that prevents information flows between Guest VMs.
		SC-4	**Information in Shared System Resources**	A conformant TOE supports this control by using virtual networks to ensure that network traffic intended for one Guest VM is not visible to any others.
		SC-7(21)	**Boundary Protection:** Isolation of System Components	A conformant TOE supports this control by ensuring that Guest VMs are isolated from one another through limitations on the extent to which data can be transferred between them.
FIA_AFL_EXT.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_UAU.5	**Multiple Authentication Mechanisms**	IA-2 -or- IA-8	**Identification and Authentication (Organizational Users)** **-or-**	A conformant TOE defines one or more mechanisms to authenticate administrators. An administrator may be an organizational or non-

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
			Identification and Authentication (Non-Organizational Users)	organizational user, depending on the mechanisms supported for authentication and the extent to which organizational resources are used to support this function.
FIA_UIA_EXT.1	**Administrator Identification and Authentication**	AC-14	**Permitted Actions Without Identification or Authentication**	A conformant TOE will limit the 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.
FMT_SMO_EXT.1	**Separation of Management and Operational Networks**	SC-2	**Separation of System and User Functionality**	A conformant TOE enforces either physical or logical separation between system (management) and user (operational) functionality.
FPT_DVD_EXT.1	**Non-Existence of Disconnected Virtual Devices**	AC-4	**Information Flow Enforcement**	A conformant TOE supports this control by implementing a mechanism that prevents information flows between Guest VMs.
		SC-4	**Information in Shared System Resources**	A conformant TOE supports this control by ensuring that a Guest VM cannot interface with a physical device it is not configured to see so that this device cannot be used as to facilitate covert communications between Guest VMs.
FPT_EEM_EXT.1	**Execution Environment Mitigations**	SI-16	**Memory Protection**	A conformant TOE has the ability to provide measures to ensure that the underlying platform's memory is protected against unauthorized code execution. The extent to which the control is satisfied depends on both the organizational safeguards that are used to mitigate this and the

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
				specific countermeasures that are used by the TOE.
FPT_HAS_EXT.1	**Hardware Assists**	SA-15(5)	**Development Process, Standards, and Tools:** Attack Surface Reduction	A conformant TOE is designed in a manner that reduces its attack surface through the use of hardware-based mechanisms that minimize the complexity of the TSF.
		SC-39(1)	**Process Isolation:** Hardware Separation	A conformant TOE supports this control through its support of hardware-based mechanisms to assist with virtualization.
FPT_HCL_EXT.1	**Hypercall Controls**	SI-3(8)	**Malicious Code Protection:** Detect unauthorized commands	A conformant TOE supports this control by ensuring that unauthorized hypercalls cannot be used to affect the behavior of the TOE through commands passed to Guest VMs.
FPT_RDM_EXT.1	**Removable Devices and Media**	AC-4	**Information Flow Enforcement**	A conformant TOE supports this control by implementing a mechanism that prevents information flows between Guest VMs.
		SC-4	**Information in Shared System Resources**	A conformant TOE supports this control by ensuring that a Guest VM cannot interact with storage media until it is no longer accessible by any other Guest VM.
FPT_TUD_EXT.1	**Trusted Updates to the Virtualization System**	CM-14	**Signed Components**	A conformant TOE requires that updates to it include integrity measures. Depending on the selection made in the SFR, this may include a digital signature.
		SI-7(1)	**Software, Firmware, and Information Integrity:** Integrity Checks	A conformant TOE has the ability to verify the integrity of updates to it.
FPT_VDP_EXT.1	**Virtual Device Parameters**	SI-3(8)	**Malicious Code Protection:** Detect unauthorized commands	A conformant TOE supports this control by ensuring that unauthorized interactions with virtual devices cannot be used to affect the behavior of the

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
				TOE through commands passed to Guest VMs.
FPT_VIV_EXT.1	**VMM Isolation from VMs**	SC-39	**Process Isolation**	A conformant TOE enforces isolation between a Guest VM, the other Guest VMs running on the virtualization system, and the virtualization system itself.
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.
FTP_ITC_EXT.1	**Trusted Channel Communications**	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_UIF_EXT.1	**User Interface: I/O Focus**	AC-4(21)	**Information Flow Enforcement:** Physical Separation of Information Flows	A conformant TOE supports this control by providing an indication of system activity. Note that the indication itself does not relate to the control being enforced; it only relates to the control to the extent that it makes the user aware of the current behavior of the TOE's information flow enforcement function.
FTP_UIF_EXT.2	**User Interface: Identification of VM**	AC-4(21)	**Information Flow Enforcement:**	A conformant TOE supports this control by providing an

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
			Physical Separation of Information Flows	indication of system activity. Note that the indication itself does not relate to the control being enforced; it only relates to the control to the extent that it makes the user aware of the current behavior of the TOE's information flow enforcement function.
Strictly Optional Requirements				
FAU_ARP.1	**Security Audit Automatic Response**	SI-4(5)	**Information System Monitoring:** System-Generated Alerts	A conformant TOE has the ability to generate alerts when system activity indicates potential unauthorized or malicious activity.
		SI-4(7)	**Information System Monitoring:** Automated Response to Suspicious Events	A conformant TOE supports part (a) of this control by implementing a mechanism to notify administrators when suspicious activity is detected.
FAU_SAA.1	**Potential Violation Analysis**	SI-4	**Information System Monitoring**	A conformant TOE supports this control by implementing a mechanism that allows it to monitor for potential unauthorized or malicious activity against itself.
FPT_GVI_EXT.1	**Guest VM Integrity**	SI-7	**Software, Firmware, and Information Integrity**	A conformant TOE supports this control by implementing a mechanism to validate the integrity of Guest VMs that are loaded into it.
		SI-7(1)	**Software, Firmware, and Information Integrity:** Integrity Checks	A conformant TOE may support this control if the integrity check performed by the TOE aligns with organizational policies for when such checks must occur.
Selection-Based Requirements				
FCS_HTTPS_EXT.1	**HTTPS Protocol**	SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE has the ability to ensure the confidentiality and integrity of information transmitted

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
				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.
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

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
				specified in part (a) of this control.
FIA_X509_EXT.1	**X.509 Certificate Validation**	IA-5(2)	**Authenticator Management:** Public Key-Based Authentication	A conformant TOE has the ability to validate certificate path and status, 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.
FIA_X509_EXT.2	**X.509 Certificate Authentication**	IA-2	**Identification and Authentication (Organizational Users)**	A conformant TOE has the ability to identify and authenticate organizational users via X.509 certificates. Other controls apply If the TOE also uses code signing certificates for software updates (CM-14, SI-7(15)) or integrity verification (SI-7, SI-7(1), SI-7(6)).
FPT_TUD_EXT.2	**Trusted Update Based on Certificates**	CM-14	**Signed Components**	A conformant TOE supports this control by using a code signing certificate to assert the integrity of software updates.
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

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
				path between remote users and itself.
Objective Requirements				
FPT_DDI_EXT.1	**Device Driver Isolation**	AC-4	**Information Flow Enforcement**	A conformant TOE supports this control by isolating device drivers from all other domains.
		SC-39	**Process Isolation**	A conformant TOE enforces isolation between its device drivers and the TOE itself so as to prevent driver errors from compromising the TOE.
FPT_IDV_EXT.1	**Software Identification and Versions**	CM-2	**Baseline Configuration**	A conformant TOE is uniquely identified through its version information in support of establishing a baseline configuration for information system assets. Note that if the TOE claims use of SWID tags in this SFR, it also supports the enforcement of CM-2(2).
		CM-8	**System Component Inventory**	A conformant TOE's use of version information supports the enforcement of this control by providing a means to uniquely identify it in an information system component inventory.
FPT_INT_EXT.1	**Support for Introspection**	SI-4	**System Monitoring**	A conformant TOE supports this control by implementing a function that allows it to monitor Guest VMs for potential malfunction or compromise.
FPT_ML_EXT.1	**Measured Launch of Platform and VMM**	SI-7(9)	**Software, Firmware, and Information Integrity:** Verify Boot Process	A conformant TOE supports this control by implementing a capability to verify the integrity of the boot process through a measured launch of the boot components.