DoD ANNEX
FOR
PROTECTION PROFILE FOR
SERVER VIRTUALIZATION (SV) V1.1

Version 1, Release 1

15 September 2015

Developed by DISA for the DoD

Trademark Information

Names, products, and services referenced within this document may be the trade names, trademarks, or service marks of their respective owners. References to commercial vendors and their products or services are provided strictly as a convenience to our users, and do not constitute or imply endorsement by DISA of any non-Federal entity, event, product, service, or enterprise.

TABLE OF CONTENTS

Page

LIST OF TABLES

1. INTRODUCTION

1.1 Background

This Annex to the Protection Profile (PP) for Server Virtualization (SV) (Version 1.1, dated 15 September 2015) delineates PP content that must be included in the Security Target (ST) for the Target of Evaluation (TOE) to be fully compliant with DoD cybersecurity policies pertaining to information systems. This content includes DoD-mandated PP selections and assignments, and PP Security Functional Requirements (SFRs) listed as objective in the PP but which are mandated in DoD.

Deficiencies of the TOE with respect to the DoD Annex will be reported as appropriate under the Risk Management Framework for DoD Information Technology (DoD Instruction 8510.01). DoD may determine that a TOE that does not conform to this Annex may pose an unacceptable risk to DoD. Accordingly, any vendor seeking authorization for use of its product within DoD should include the additional PP specificity described in this Annex in its ST.

The PP for SV, in conjunction with this Annex, addresses the DoD-required cybersecurity controls in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53.

1.2 Scope

The additional information in this document is applicable to all DoD-administered systems and all systems connected to DoD networks.

1.3 Relationship to Security Technical Implementation Guides (STIGs)

A successful Common Criteria evaluation certifies the capabilities of the TOE but does not assure its subsequent secure operation. To address security concerns with the ongoing operation of the TOE in the field, a product-specific STIG is prepared in conjunction with the Common Criteria evaluation. The STIG lists the configuration requirements for DoD implementations of the TOE and is published in eXtensible Configuration Checklist Description Format (XCCDF) to facilitate automation where feasible.

This Annex contains the required DoD configuration of features implementing the security management (FMT) class of SFRs listed in the PP for Server Virtualization. For each applicable FMT SFR, the STIG will discuss the vulnerability associated with non-compliance configuration and provide step-by-step, product-specific procedures for checking for compliant configurations and fixing non-compliant configurations.

In most cases, the ST will not cover all security-relevant configurable parameters available in the TOE. However, the STIG will include these whenever they impact the security posture of DoD information systems and networks. Accordingly, the DoD Annex only addresses a subset of the controls expected to be included in a STIG.

1.4 Document Revisions

Comments or proposed revisions to this document should be sent via email to: disa.stig_spt@mail.mil.

2. DOD-MANDATED SECURITY TARGET CONTENT

The following conventions are used to describe DoD-mandated ST content:

- If a PP SFR is not listed, there is no DoD-mandated selection or assignment for that SFR.
- For PP selections:
  - The presence of the selection indicates this is a DoD-mandated selection.
  - If a selection is not listed, then its inclusion or exclusion does not impact DoD compliance.
  - Underlined text indicates a selection.
  - *Italicized and underlined* text indicates an assignment within a selection.
  - ~~Strikethrough~~ text indicates that the ST author must exclude the selection.
- For PP assignments:
  - The DoD-mandated assignments are listed after the assignment parameter.
  - If an assignment value appears in ~~strikethrough~~ text, this indicates that the assignment must not include this value.
  - *Italicized* text indicates an assignment.

The Annex provides the minimum text necessary to disambiguate selections and assignments. Readers will need to view both the PP for SV and the DoD Annex simultaneously to place the Annex information in context.

2.1 DoD-Mandated Assignments and Selections

DoD mandates the following PP SFR assignments and selections for SFRs in Section 5 of the PP for SV:

Table 2-1: PP SFR Selections

SFR	Selections, Assignments, and Application Notes
FAU_GEN.1.1	Specifically defined auditable events listed in Table 8.
FAU_STG_EXT.1.2	~~drop new audit data~~. *overwrite the oldest audit records in a first-in-first-out manner shut down if availability concerns can be addressed by migrating guest VMs to other hosts*; *drop old audit data already sent to an external audit/logging server*. Application note: The assignments enumerated here are provided as alternatives acceptable to the DoD. Not all must be implemented.
FDP_PPR_EXT.1.1	*removable media; external devices*.
FIA_UIA_EXT.1.1	*Display advisory warning banner in support of FTA_TAB.1*
FIA_X509_EXT.2.1	code signing for system software updates; code signing for integrity verification.
FIA_X509_EXT.2.2	~~accept the certificate~~.

SFR	Selections, Assignments, and Application Notes
FMT_MOF_EXT.1.1	2. digital signature 12. Ability to configure the list of TOE_provided services available before an entity is identified and authenticated, as specified in FIA_UIA_EXT.1; Ability to configure the cryptographic functionality; Ability to change default authorization factors; Ability to enable/disable screen lock; Ability to configure screen lock inactivity timeout; Ability to configure remote connection inactivity timeout; Ability to configure lockout policy for unsuccessful authentication attempts; Ability to configure name/address of directory server to bind with; Ability to configure name/address of audit/logging server to which to send audit/logging records; Ability to configure name/address of network time server; *Limiting number of attempts during a time period*.
FMT_MOF_EXT.1.2	~~unprivileged Users~~. Application note: Some virtualization system use cases may require that unprivileged Users have the ability to manipulate VMs. It is expected that these activities will be mediated through some type of control mechanism external to the virtualization system to ensure that VMs of other unprivileged Users can not be manipulated without prior authorization.
FPT_TUD_EXT.1.2	support automatic updates.
FPT_TUD_EXT.1.3	digital signature mechanism.

2.2 DoD-Mandated Optional, Selection-Based, and Objective SFRs

The following SFRs listed as optional or objective in the PP are mandated for the DoD:

- FPT_TUD_EXT.2.1
- FTA_TAB.1
- FPT_INT_EXT.1.1
- FPT_DDI_EXT.1.1

3. OTHER DOD MANDATES

3.1 Federal Information Processing Standard (FIPS) 140-2

Cryptographic modules supporting any SFR in the Cryptographic Support (FCS) class must be FIPS140-2 validated. While information concerning FIPS 140-2 validation should not be included in the ST, failure to obtain validation could preclude use of the TOE within DoD.

3.2 Federal Information Processing Standard (FIPS) 201-2

The TOE is expected to interface with FIPS 201-2 compliant credentials (to include derived credentials as described in NIST Special Publication 800-157). The TOE may connect to a peripheral device (e.g., a smart card reader) in order to interface with PIV credentials, or natively store derived credentials (whose protections are evaluated in the Protection Profile).

3.3 DoD-Mandated Configuration

The table below lists configuration values for product features implementing the PP Specification of Management Functions (FMT_SMF). The ST is not expected to include this configuration information, but it will be included in the product-specific STIG associated with the evaluated IT product. Non-binary configuration values are shown in *italics*.

Table 3-1: Configuration Values

FMT_MOF_EXT.1.1 Function	DoD Selections and Values
Function 3	minimum password length = *15 characters* minimum password complexity = *at least 1 lowercase character; at least 1 uppercase character; at least 1 numeric character; at least 1 special character; change at least 50% of characters in password when it is updated; at least 5 generations of password updates before reuse* maximum password lifetime = *60 days* Application note: The PP does not provide selections for password complexity. Therefore, the DoD-mandated complexity rule described above is not included in the PP. Vendors must either provide the capability to support this rule or justify why an alternative supported complexity scheme offers equivalent or stronger protection against the vulnerability of easily guessed or simple passwords.
Function 12	Advisory warning message (one of the following) = For devices accommodating advisory warning messages of 1300 characters: *You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.* *By using this IS (which includes any device attached to this IS), you consent to the following conditions:* *-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.* *-At any time, the USG may inspect and seize data stored on this IS.* *-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.* *-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.* *-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.* *-Notwithstanding the above, using this IS does not constitute consent to PM, LE, or CI investigative searching or monitoring of the content of privileged communications, or work product, related*

	to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details. For servers with severe character limitations: *I've read & consent to terms in IS user agreem't.* screen lock enabled screen lock inactivity timeout = *15 minutes or less* lockout policy for unsuccessful authentication attempts = limited to *3* attempts during a *15* minute time period remote connection inactivity timeout = *15 minutes or less*