

UNCLASSIFIED



# **VIRTUAL MACHINE MANAGER (VMM) SECURITY REQUIREMENTS GUIDE (SRG) TECHNOLOGY OVERVIEW**

**Version 2, Release 1**

**24 July 2024**

**Developed by DISA for the DOD**

UNCLASSIFIED

### **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 the Defense Information Systems Agency (DISA) of any nonfederal entity, event, product, service, or enterprise.

TABLE OF CONTENTS

	Page
<b>1. INTRODUCTION .....</b>	<b>1</b>
1.1 Executive Summary.....	1
1.1.1 Security Requirements Guides (SRGs) .....	1
1.1.2 SRG Naming Standards .....	2
1.2 Authority.....	2
1.2.1 Relationship to STIGs .....	3
1.3 Vulnerability Severity Category Code Definitions .....	3
1.4 SRG and STIG Distribution.....	3
1.5 Document Revisions .....	3
1.6 Other Considerations .....	4
1.7 Product Approval Disclaimer .....	4
<b>2. ASSESSMENT CONSIDERATIONS .....</b>	<b>5</b>
2.1 NIST SP 800-53 Requirements.....	5
2.2 General Procedures .....	5

LIST OF TABLES

	<b>Page</b>
Table 1-1: Vulnerability Severity Category Code Definitions .....	<b>3</b>

## 1. INTRODUCTION

### 1.1 Executive Summary

This Virtual Machine Manager (VMM) Security Requirements Guide (SRG) provides the technical security policies and requirements for applying security concepts to systems.

This SRG specifies security requirements for VMMs providing full-system virtualization services in a networked environment on server-class hardware. A VMM may be fielded as a standalone operating system (bare-metal VMM) or as a VMM application on a general-purpose operating system; in the latter case, the host operating system may satisfy some VMM SRG requirements in support of the VMM application. Full-system virtualization creates a virtualized hardware environment for each instance of a virtualized operating system (virtual machine or guest VM).

All VMM management interfaces and APIs are within the scope of this SRG, although external applications utilizing the management APIs may not be fully within scope. All references to “users” and “accounts” refer to entities operating with the VMM itself; users and accounts of guest VMs are managed in the context of the guest VMs themselves. Distinctions are also made for “local” users and accounts, which are provisioned on and by the VMM itself, as opposed to users and accounts provisioned by an enterprise account management infrastructure. This SRG does not address operating system virtualization, such as chroot jails or Solaris containers. It also does not address application virtualization, such as that provided by a Java virtual machine. Guest VMs not directly supporting VMM functions are to be evaluated as standalone systems and are outside of scope. This SRG assumes operation in a single security domain. Cross-domain solution (CDS) and Multi-level Secure (MLS) requirements are outside of scope.

#### 1.1.1 Security Requirements Guides (SRGs)

Security Requirements Guides are collections of requirements applicable to a given technology family. They represent an intermediate step between Control Correlation Identifiers (CCIs) and Security Technical Implementation Guides (STIGs). CCIs represent discrete, measurable, and actionable items sourced from Information Assurance (IA) controls defined in a policy, such as the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53. STIGs provide product-specific information for validating and attaining compliance with requirements defined in the SRG for that product’s technology area.

There are four core SRGs: Application, Network, Operating System, and Policy. Each addresses the applicable CCIs in the context of the technology family. Subordinate to the core SRGs, there are Technology SRGs developed to address the technologies at a more granular level.

The VMM SRG is based on the Operating System core SRG. This VMM SRG contains general check and fix information that can be utilized for products for which STIGs do not exist.

The STIGs based on this SRG will provide the product-specific technical implementation guidance for that product. The STIG will contain the specific check and fix information for the product it covers.

**SRG Hierarchy example:**

```

Application SRG
|__Database SRG
    |__MS SQL Server 2005 STIG

```

The SRG relationship and structure provides the ability to identify requirements that may be considered not applicable for a given technology family and provide appropriate justification. It also provides the structure to identify variations in specific values based on the technology family. These variations will be captured once and will propagate down to the Technology SRGs and then to the STIGs. This will eliminate the need for each product-specific STIG to address items that are not applicable.

**1.1.2 SRG Naming Standards**

In an effort to establish consistency across the SRGs, a naming standard for the Group Title and STIGIDs has been established.

**Technology SRG Naming Standards**

For Technology SRG Group Title and STIGIDs the following applies:

*{Core SRG value}-{Technology SRG}-{5- or 6-digit numeric sequence number}*

Examples:

```

SRG-NET-000001-RTR-000001
SRG-APP-000001-COL-000001
SRG-NET-000001-VVSM-00001
SRG-OS-000001-UNIX-000001

```

Checks/Fixes will be included at this level in a general form. These checks and fixes will apply for any STIGs that are created for products that do not have product-specific check and fix guidance.

**1.2 Authority**

Department of Defense Instruction (DODI) 8500.01 requires that “all IT [information technology] that receives, processes, stores, displays, or transmits DOD information will be [...] configured [...] consistent with applicable DOD cybersecurity policies, standards, and architectures.” The instruction tasks that DISA “develops and maintains control correlation identifiers (CCIs), security requirements guides (SRGs), security technical implementation guides (STIGs), and mobile code risk categories and usage guides that implement and are consistent with DOD cybersecurity policies, standards, architectures, security controls, and validation procedures, with the support of the NSA/CSS [National Security Agency/Central Security Service], using input from stakeholders, and using automation whenever possible.” This document is provided under the authority of DODI 8500.01.

Although the use of the principles and guidelines in these SRGs/STIGs provides an environment that contributes to the security requirements of DOD systems, applicable NIST SP 800-53 cybersecurity controls must be applied to all systems and architectures based on the Committee on National Security Systems (CNSS) Instruction (CNSSI) 1253.

### 1.2.1 Relationship to STIGs

The SRG defines the requirements for various technology families, and the STIGs are the technical implementation guidelines for specific products. A single SRG/STIG is not all-inclusive for a given system, which may include but is not limited to Database, Web Server, and Domain Name System (DNS) SRGs/STIGs. For a given system, compliance with all (multiple) SRGs/STIGs applicable to a system is required.

## 1.3 Vulnerability Severity Category Code Definitions

Severity Category Codes (referred to as CAT) are a measure of vulnerabilities used to assess a facility or system security posture. Each security policy specified in this document is assigned a Severity Category Code of CAT I, II, or III.

**Table 1-1: Vulnerability Severity Category Code Definitions**

	DISA Category Code Guidelines
CAT I	Any vulnerability, the exploitation of which will <b>directly and immediately</b> result in loss of Confidentiality, Availability, or Integrity.
CAT II	Any vulnerability, the exploitation of which <b>has a potential</b> to result in loss of Confidentiality, Availability, or Integrity.
CAT III	Any vulnerability, the existence of which <b>degrades measures</b> to protect against loss of Confidentiality, Availability, or Integrity.

## 1.4 SRG and STIG Distribution

Parties within the DOD and federal government's computing environments can obtain the applicable STIG from the DOD Cyber Exchange website at <https://cyber.mil/>. This site contains the latest copies of STIGs, SRGs, and other related security information. Those without a Common Access Card (CAC) that has DOD Certificates can obtain the STIG from <https://public.cyber.mil/>.

## 1.5 Document Revisions

Comments or proposed revisions to this document should be sent via email to the following address: [disa.stig\\_spt@mail.mil](mailto:disa.stig_spt@mail.mil). DISA will coordinate all change requests with the relevant DOD organizations before inclusion in this document. Approved changes will be made in accordance with the DISA maintenance release schedule.

## 1.6 Other Considerations

DISA accepts no liability for the consequences of applying specific configuration settings made on the basis of the SRGs/STIGs. It must be noted that the configuration settings specified should be evaluated in a local, representative test environment before implementation in a production environment, especially within large user populations. The extensive variety of environments makes it impossible to test these configuration settings for all potential software configurations.

For some production environments, failure to test before implementation may lead to a loss of required functionality. Evaluating the risks and benefits to a system's particular circumstances and requirements is the system owner's responsibility. The evaluated risks resulting from not applying specified configuration settings must be approved by the responsible AO. Furthermore, DISA implies no warranty that the application of all specified configurations will make a system 100 percent secure.

Security guidance is provided for the DOD. While other agencies and organizations are free to use it, care must be given to ensure that all applicable security guidance is applied at both the device hardening level and the architectural level due to the fact that some settings may not be configurable in environments outside the DOD architecture.

## 1.7 Product Approval Disclaimer

The existence of a STIG does not equate to DOD approval for the procurement or use of a product.

STIGs provide configurable operational security guidance for products being used by the DOD. STIGs, along with vendor confidential documentation, also provide a basis for assessing compliance with cybersecurity controls/control enhancements, which supports system assessment and authorization (A&A) under the DOD Risk Management Framework (RMF). Department of Defense AOs may request available vendor confidential documentation for a product that has a STIG for product evaluation and RMF purposes from [disa.stig\\_spt@mail.mil](mailto:disa.stig_spt@mail.mil). This documentation is not published for general access to protect the vendor's proprietary information.

AOs have the purview to determine product use/approval in accordance with (IAW) DOD policy and through RMF risk acceptance. Inputs into acquisition or pre-acquisition product selection include such processes as:

- National Information Assurance Partnership (NIAP) evaluation for National Security Systems (NSS) (<https://www.niap-ccevs.org/>) IAW CNSSP #11.
- National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) (<https://csrc.nist.gov/groups/STM/cmvp/>) IAW federal/DOD mandated standards.
- DOD Unified Capabilities (UC) Approved Products List (APL) (<https://www.disa.mil/network-services/ucco>) IAW DODI 8100.04.



## **2. ASSESSMENT CONSIDERATIONS**

### **2.1 NIST SP 800-53 Requirements**

All applicable baseline technical NIST SP 800-53 requirements and security best practice requirements are included in this SRG.

CNSSI 1253 defines the required controls for DOD systems, based on confidentiality, integrity, and availability (baseline) of the given information system. In all cases, CNSSI 1253, along with required baselines, will serve as the policy requirement for any given asset or information system.

### **2.2 General Procedures**

This SRG has procedures that are intended to provide appropriate evaluation and remediation functions for a typically configured system. These procedures are not product specific and are intended for use when a product-specific STIG is not available.