Sun Ray
SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG) OVERVIEW

Version 1, Release 2

24 April 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

1. INTRODUCTION 1

1.1 Executive Summary 1
1.2 Authority 1
1.3 Vulnerability Severity Category Code Definitions 1
1.4 STIG Distribution 2
1.5 SRG Compliance Reporting 2
1.6 Document Revisions 2

2. ASSESSMENT CONSIDERATIONS 3

2.1 Command Examples 3
2.2 Alternate Software 3
2.3 Requirements for Disabled Functions 3

3. SOFTWARE PATCHING GUIDELINES 4

LIST OF TABLES

Page

Table 1-1: Vulnerability Severity Category Code Definitions 2

1. INTRODUCTION

1.1 Executive Summary

The Sun Ray Security Technical Implementation Guide (STIG) is published as a tool to improve the security of Department of Defense (DoD) information systems. The requirements were developed from Federal and DoD consensus and items sourced from Information Assurance (IA) controls defined in policy such as those originating in Department of Defense (DoD) Instruction (DoDI) 8500.2 and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53. STIGs provide product-specific information for validating and attaining compliance.

1.2 Authority

DoD Instruction (DoDI) 8500.01 requires that "all IT that receives, processes, stores, displays, or transmits DoD information will be […] configured […] consistent with applicable DoD cybersecurity policies, standards, and architectures" and tasks that Defense Information Systems Agency (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, 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 provide an environment that contributes to the security requirements of DoD systems, applicable NIST SP 800-53 cybersecurity controls need to be applied to all systems and architectures based on the Committee on National Security Systems (CNSS) Instruction (CNSSI) 1253.

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 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, **directly and immediately** result in loss of Confidentiality, Availability, or Integrity.
CAT II	Any vulnerability, the exploitation of which **has a potential** to result in loss of Confidentiality, Availability, or Integrity.
CAT III	Any vulnerability, the existence of which **degrades measures** to protect against loss of Confidentiality, Availability, or Integrity.

1.4 STIG Distribution

Parties within the DoD and Federal Government's computing environments can obtain the applicable STIG from the Information Assurance Support Environment (IASE) website. This site contains the latest copies of any STIGs, SRGs, and other related security information. The address for the IASE site is http://iase.disa.mil/.

1.5 SRG Compliance Reporting

All technical NIST SP 800-53 requirements were considered while developing this STIG. Requirements that are applicable and configurable will be included in the final STIG. A report marked For Official Use Only (FOUO) will be available for those items that did not meet requirements. This report will be available to component Authorizing Official (AO) personnel for risk assessment purposes by request via email to: disa.stig_spt@mail.mil.

1.6 Document Revisions

Comments or proposed revisions to this document should be sent via email to the following address: 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.

2. ASSESSMENT CONSIDERATIONS

2.1 Command Examples

Some check and fix procedures contain example commands that can be used to obtain information regarding compliance with a requirement or to change a setting to attain compliance with a requirement. These example commands assume use of a standard UNIX shell operating as the root user. If the software used by these commands is not present on the system, the system administrator (SA) or the reviewer is responsible for determining compliance with the requirement using the tools available on the system. Check procedures also contain instructions for evaluating compliance based on the output of these commands.

2.2 Alternate Software

Sun Ray systems offer flexibility in replacing, adding to, and enhancing components provided by Oracle with other software to meet operational needs. Many of the check and fix procedures in the Sun Ray STIG assume the use of the software provided by Oracle. If alternate software is used to provide a function ordinarily provided by a default system application, the specific check and fix information for that function is no longer valid. The SA or the reviewer is responsible for evaluating the requirements based on documentation available for the alternate software. The system accreditation package must contain information pertaining to the use of alternate software.

2.3 Requirements for Disabled Functions

The Sun Ray STIG defines requirements for the further hardening and configuration of system functions that are required to be disabled. These requirements exist to address vulnerabilities in the system resulting from accidental activation, malicious intentional activation, or intentional activation of the system function based on acceptance of risk by the Authorizing Official (AO). Requirements for a system function remain applicable even when the system function is disabled. Requirements pertaining to software that is not installed on the system, and which has no remaining configuration files on the system, may be evaluated as Not Applicable (NA).

3. SOFTWARE PATCHING GUIDELINES

Maintaining the security of a Sun Ray system requires frequent reviews of security bulletins. Many security bulletins and IAVM notifications mandate the installation of software patches to overcome noted security vulnerabilities. The SA will be responsible for installing all such patches. The Information System Security Officer (ISSO) will ensure the vulnerabilities have been remedied. DISA guidelines for remediation, including IAVMs, are as follows:

- Apply the applicable patch, upgrade to required software release, or remove the binary/application to remediate the finding.
- Or, the mode of the vulnerable binary may be changed to 0000 to downgrade the finding (for example, a CAT I finding may be downgraded to a CAT II).

SAs and ISSOs will regularly check Oracle's vendor and third-party application vendor websites for information on new vendor-recommended updates and security patches that are applicable to their site. All applicable vendor-recommended updates and security patches will be applied to the system. A patch is deemed applicable if the product is installed, even if it is not used or is disabled.