ORACLE DATABASE 12c
SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG)
OVERVIEW

Version 2, Release 5

27 July 2022

Developed by Oracle and DISA for the DoD

Trademark Information

TABLE OF CONTENTS

Page

LIST OF TABLES

Page

1. INTRODUCTION

1.1 Executive Summary

The Oracle Database 12c Security Technical Implementation Guide (STIG) is published as a tool to improve the security of Department of Defense (DoD) information systems. This document is meant for use in conjunction with the Enclave, Network Infrastructure, Secure Remote Computing, and appropriate Operating System (OS) STIGs. It is based on the Database Security Requirements Guide (SRG) Version 1 Release 1, which in turn derives its cybersecurity controls from National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 3.

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.

1.3 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 **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 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 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 Controlled Unclassified Information (CUI) will be available for 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.

1.7 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.

1.8 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. 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. CONCEPTS AND TERMINOLOGY CONVENTIONS

2.1 Oracle Database 12c

Oracle Database 12c is a relational Database Management System (DBMS), together with associated software tools, some of which come bundled with the DBMS, and some as separate products.

Oracle was the first commercially available relational DBMS. It came to market in 1979. Since then, it has developed into a robust, highly scalable product with a rich feature set and a large collection of associated tools and applications. In the same timeframe, the relational model has become the standard architecture for general-purpose databases.

The typical smaller Oracle deployment consists of one instance of the DBMS software servicing one database (a collection of data, stored in files and managed, not by the OS alone, but by the DBMS). Larger, clustered deployments have multiple instances of the DBMS software, each running on its own server, and typically servicing a single, shared database housed on dedicated storage systems. (This contrasts with some other DBMS brands, where software instances, single or clustered, can and often do support multiple databases).

The language used for data definition, data manipulation, security management, etc., is Structured Query Language (SQL). Oracle extends this declarative language with Procedural Language/Structured Query Language (PL/SQL), which provides the full power of a programming language within the database itself. Programs written in PL/SQL are known as stored procedures. Java can also be used to create stored procedures.

Applications communicate with Oracle by sending it SQL or PL/SQL commands—usually known as queries—that typically are invocations of stored procedures. Applications can be written in any language capable of handling Oracle's interface conventions. Applications may run on the same server as the DBMS, but typically—and especially in the DoD—will run on dedicated web servers or client machines.