DATABASE
SECURITY REQUIREMENTS GUIDE (SRG)
TECHNOLOGY OVERVIEW

Version 2, Release 4

22 April 2016

Developed by DISA for the DoD

Trademark Information

TABLE OF CONTENTS

Page

LIST OF TABLES

Page

1. INTRODUCTION

1.1 Executive Summary

This Database Security Requirements Guide (SRG) provides the technical requirements for applying security concepts to database management systems (DBMS) and databases. While some of the entries refer to policy requirements, as a technical SRG, this document does not go into depth with respect to policy: that is the purview of the Policy SRG.

This SRG addresses all IA Controls from NIST SP 800-53, Revision 4 that have been selected for the DoD baseline and have not been determined to be fully covered by the guidance for another technology area.

Note that one class of policy requirement covers the topic of organization-defined values. Wherever this document refers to "organization-defined" values, it is assuming that the values have been defined at the appropriate organizational level, covering the system under review. By contrast, values that have been decided upon for the whole of DoD are explicitly stated in this SRG.

1.1.1 Security Requirements Guides (SRGs)

SRGs are collections of requirements applicable to a given technology family. SRGs 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.

This Database SRG is based on the Application SRG. This Database SRG contains general check and fix information that can be utilized for products for which STIGs do not exist.

Each STIG based on this SRG will provide the technical implementation guidance for one DBMS 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 2012 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}-{6-digit numeric sequence number}

Examples:

SRG-NET-000001-RTR-000001
SRG-APP-000001-COL-000001
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

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 provides 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.

1.2.1 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 **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 SRG and 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 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.

1.6 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 Authorizing Official. 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 Department of Defense. While other agencies and organizations are free to use it, care must be given to ensure that all applicable security guidance is applied both at the device hardening level as well as the architectural level due to the fact that some of the settings may not be able to be configured 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). DoD Authorizing Officials (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 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) (http://www.niap-ccevs.org/) IAW CNSSP #11
- National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) (http://csrc.nist.gov/groups/STM/cmvp/) IAW Federal/DoD mandated standards
- DoD Unified Capabilities (UC) Approved Products List (APL) (http://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.

The Database SRG identifies potential vulnerabilities that undermine security, contribute to inefficient operations and administration, or may lead to interruption of production operations. Reviews are done to ensure the database environment is secure, efficient, and effective.

The security requirements contained within the Database SRG are applicable to all DoD-administered systems and all systems connected to DoD networks. The Database SRG provides requirements and associated procedures to reduce the security vulnerabilities of any DBMS products not covered under a product-specific Database STIG. These requirements are designed to assist SMs, ISSMs, ISSOs, SAs, and DBAs with configuring and maintaining security controls in a generic DBMS.

As with many applications, there may be multiple ways to perform a vulnerability assessment. This document is not intended to provide all check procedure variations; it is designed to provide at least one way to check and fix a vulnerability.

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.

3. CONCEPTS AND TERMINOLOGY CONVENTIONS

3.1 Database Technology Overview

A DBMS may provide capabilities that control or affect the security of the data stored within its files. DBMS security capabilities include:

- Authentication – a DBMS may provide its own authentication mechanism or use the host operating system or another external authentication system such as a directory service to identify and authenticate users. This SRG prescribes use of the latter method.
- Authorization – a DBMS provides three types: 1) privileges that protect data and objects definition; 2) privileges that control access to the data stored within the database objects; and 3) privileges to administer the database configuration and operation behaviors.
- Confidentiality – a DBMS may provide data encryption for stored and communicated data.
- Integrity – a DBMS typically provides data validation mechanisms, data relationship integrity, transaction logging and rollback, and session lock mechanisms to control multiple update requests against the same data.
- Audit – a DBMS may provide configurable audit logging of actions taken.
- Backup and Recovery – a DBMS typically provides backup and recovery features to mitigate hardware or software failure losses.

Applications may also require that the database take advantage of one or more of the following remote database features:

- Replication – part or all of the database data objects may be copied and maintained in a separate remote database.
- Federated or distributed databases – these provide access to data stored in remote databases to local database users and applications.
- Database clustering – database clustering provides high-availability to data by providing instant access to duplicate databases in the event of access failure to a primary database.

Database security also depends on supporting environments such as:

- The host operating system – provides protection of the database and its configuration data.
- The application – provides access to the data. If the application does not contribute to the security model, it can provide fully-privileged, un-audited access to the database and data to which it connects.
- The network – provides protections via network devices and applications.
- Web and/or application servers – provide the security framework for all hosted web applications; these servers may control access to other served applications.

These elements collectively contribute to the overall security posture of the database.

3.2 Authentication

Identification and authentication (I&A) features provide the foundation for access control. A DBMS may provide mechanisms for identifying and authenticating users. Users are identified to the database with a user account, which may be defined in the host operating system, a directory service, a network authentication service, or the database itself. The DBMS is likely to support multiple authentication methods, including passwords, certificates, and tokens.

Most databases support username/password authentication. Password management includes configuring mandatory password specifications for complexity, reuse, expiration, and screen obfuscation.

DBMS products that support certificate authentication method must be carefully configured to meet certificate validation and protection requirements. Self-signed certificates are not a recommended practice.

Note that this SRG discourages the use of DBMS native I&A and the use of user names and passwords. It includes requirements that all DBMS/database accounts (users; roles/groups) be managed by an organization-wide directory service implementing the Public Key Infrastructure (PKI). This is the rationale for the SRG's not directly addressing most of the NIST SP 800-53 Information Assurance (IA) controls regarding account management: they are covered by the guidance for the directory service.

3.3 Database user accounts

Database accounts can, and should, be mapped to external authentication services, including directory servers (as noted in the previous section), operating system, Kerberos, or other accounts. (The alternative is for all accounts and roles to be managed by the DBMS alone, a practice forbidden by this SRG.) The database account name may or may not be the same as the external account name. A given account is a member of one or more roles/groups, which simplify the administration of permissions. Examples of database roles are:

- Application User – an interactive user who requires only access to read (select), insert, update, or delete data in existing database tables. These are referred to as Database Manipulation Language (DML) actions.
- Database Administrator (DBA) – the responsible account category for configuring and operating the database. The DBA account has full privileges to all objects and resources in the database, including user accounts.
- Application Owner – owns all objects defined and used by an application. The application owner defines application roles and assigns user object privileges to the application objects to the application roles. Application owner privileges are restricted to creation, deletion (dropping), or altering of database objects (commonly referred to as Database Definition Language (DDL) actions).
- Application User Manager – may create and manage application users within the database, including roles assignments.

- Application Account – a specialized user account for an application, a service, or local batch job. An application account may have permissions tailored to access specific system objects.
- Database Auditor – a specialized user account for audit records management. Use of a database auditor account enables roles separation where alternate permissions are desirable. With a separate account assignment, auditor actions may be assigned and monitored with appropriate (non-administrator) permissions.
- Database Operator – a specialized user account for startups, backups, and restore operations. Use of an operator account enables roles separation where alternate permissions are desirable. With a separate account assignment, operator actions may be assigned and monitored with appropriate (non-administrator) permissions.

Unmanaged database accounts may provide opportunity for mischief. Use of automated controls, such as account locking after failed logon attempts, can help protect against unauthorized access attacks.