SQL SERVER 2012
SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG) OVERVIEW

Version 1, Release 16

26 January 2018

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 Document Revisions 2
1.6 Other Considerations 2
1.7 Product Approval Disclaimer 3

2. ASSESSMENT 4

2.1 General Information 4
2.2 Security Assessment Information 4
2.3 Temporary Tables 4
2.4 Run Time 4

3. CONCEPTS AND TERMINOLOGY CONVENTIONS 5

3.1 Third-Party Tools 5

LIST OF TABLES

Page

Table 1-1: Vulnerability Severity Category Code Definitions 2

1. INTRODUCTION

1.1 Executive Summary

The SQL Server 2012 Overview, along with the SQL Server 2012 Security Technical Implementation Guide (STIG), provides the technical security policies, requirements and implementation details for applying security concepts to Microsoft SQL Server 2012. This document is meant to improve the security of Department of Defense (DoD) information systems. The requirements in the accompanying STIG do not necessarily prevent or mitigate all attacks against a poorly designed application which uses SQL Server. Please refer to the Application Security and Development STIG for application requirements. Consideration must be given to the placement of SQL server inside a forest to ensure evaluation of risk within the environment is considered. Risk includes introduction of risk to SQL Server from other applications or workstations as well as risk from introduction of SQL server itself into an established environment.

Please note additional guidance exists that applies to SQL Server, even though it is non-SQL-specific and therefore not explicitly called out in the SQL Server 2012 STIG. This includes the Windows environment as well as the networking requirements including firewall protection, DMZ requirements, and Windows host requirements.

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.

1.3 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 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

2.1 General Information

The security requirements contained within the SQL Server 2012 STIG are broken into two parts. The SQL Server Instance STIG will be used for the setting to apply to the actual instance (or installation) of SQL Server 2012. The SQL Server 2012 Database STIG should be used for each individual database (including those that are vendor-supplied, such as master).

2.2 Security Assessment Information

The execution of the manual procedures may require Administrator (Windows Server) and SQL Server DBA privileges in both the system database and user-defined database instances. This may vary based on the permissions assigned to the account used. It is expected that an authorized DBA or the ISSO log and monitor this account. It is assumed that SQL Server 2012 is running on a version of Windows Server 2008 or later.

2.3 Temporary Tables

Some of the queries that are in the checks of this STIG create temporary files in order to do the check. These temporary files are all deleted by the query, if successful (without a runtime error). Also, the temporary files, if they exist, are deleted near the beginning of each query that creates temporary files. The query should not generate a “table already exists” error if the query did not complete successfully on a previous execution.

2.4 Run Time

Running the queries could have an impact on the database performance based on the priority of the queries and the number of database objects. For example, the number of users can affect the permissions queries. If queries run with a hit priority, as most DBA accounts do, the assessment queries could interfere with successful processing by regular users. If this occurs, using a lower account priority, or running SQL queries during SQL Server lower service times could reduce or eliminate the effects to regular users.

3. CONCEPTS AND TERMINOLOGY CONVENTIONS

This section describes concepts, such as third-party tools and data labeling. These terms and concepts are relevant throughout the SQL Server 2012 STIG. If a term or concept is specific to a single vulnerability, then the term or concept is explained within that vulnerability.

3.1 Third-Party Tools

The SQL Server 2012 STIG has many references to third-party tools. These third-party tools are assumed to satisfy a specific functionality quickly and easily without a large SQL scripting development effort. For example, one requirement asks for real-time viewing of a user session, and an example solution was given using the SQL Server "fn_get_audit_file" function. However, there are existing third-party tools that can view audit file information in a GUI format, while reducing extraneous data.

Though there are many references to third-party tools within the SQL Server 2012 STIG, almost none are mentioned by name, except those that Microsoft provides directly, e.g., Security Labeling via Codeplex.