SHAREPOINT SERVER 2010
SECURITY TECHNICAL IMPLEMENTATION GUIDE
(STIG) OVERVIEW

Version 1, Release 7

23 October 2015

Developed by DISA for the DoD

Trademark Information

TABLE OF CONTENTS

Page

LIST OF TABLES

Page

1. INTRODUCTION

1.1 Executive Summary

The SharePoint Server 2010 Security Technical Implementation Guide (STIG) provides guidance for secure configuration and usage of Microsoft's SharePoint implementation. The STIG provides security guidance for SharePoint deployments in a single server or server farm consisting of multiple servers. This overview document gives technology-specific background and information on conducting a security review for SharePoint 2010 Server. SharePoint Foundation and previous versions of SharePoint are not addressed, although there is significant overlap in the security impacts for these products.

SharePoint 2010 requires 64-bit hardware for each server in the farm, including the database server, and therefore requires 64-bit versions of Windows and Microsoft SQL (Structured Query Language) Server. Windows Server 2008 is the minimum Operating System (OS) version for production servers.

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 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 configurations 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% 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.

2. TECHNOLOGY

This section provides background information on Microsoft SharePoint Services and discusses general security considerations involved with using this technology.

This overview document is not intended as a comprehensive source of information on SharePoint. Microsoft and many other authors have produced a lot of documentation and many books are available for reference. Additionally, this STIG is not intended as a tutorial or training tool for inexperienced SAs. Since SharePoint is an integrated product which leverages a number of outside services, knowledge of the Windows OS, AD, SQL, and IIS Internet Information Services software is a prerequisite to understanding how to use the SharePoint STIG requirements.

2.1 Topology

SharePoint can be deployed on single server or multiple servers. However, DoD implementations of SharePoint must be installed in a farm configuration rather than a single server configuration. The single server configuration installs the SQL database on the application server which is a violation of DoD least privilege policy.

There are three (3) minimum roles required in SharePoint farm architecture: the Web Server role, the Application Server role, and the Database Server role. In smaller farms, the role of Web Server and Application Server may be combined. In large server farms, multiple servers may exist for each role. These servers allow for load balancing and redundancy.

Web server role:

- Hosts web pages, web services, and web parts which receive and initially process the requests to SharePoint.
- Passes the service requests to appropriate application server.

Application server role:

- The application server role hosts SharePoint services. Services can be distributed or grouped on application servers. Individual services can installed onto a dedicated application server, (e.g., to implement load balancing or separation of services), as required by the organizationally-determined information flow plan.
- Client-related services are based on usage, and should be deployed to separate servers by usage.
- Services with external connections should be deployed onto separate application servers than those with only internal connections.

Database server role:

- There are three (3) broad database categorizations: Search Databases, Content Databases, and Service Databases.

  - Service Databases include business data connectivity, user profile data, usage and health data collection, and state service.
  - Search databases support crawling content sources and end-user queries. There are tables and indexes in the database that are used just for crawling; other tables and indexes are used for end-user queries but are updated by the crawling process.
  - Content databases store and manage SharePoint site content. Just as each virtual server can host multiple top-level Web sites, each virtual server can rely on multiple content databases to store site content. These databases can be shared across the farms depending on size and usage.
- In a small farm, a single server could be deployed to host all types of content.

In large farms, the recommendation is to group the databases by roles and deploy them to multiple database servers.

2.2 Product Dependencies

SharePoint service and user data content are stored in a SQL database server. Following are the minimum SQL server Database versions:

- The 64-bit edition of Microsoft SQL Server 2008 R2.
- The 64-bit edition of Microsoft SQL Server 2008 with Service Pack 1 (SP1).
- The 64-bit edition of Microsoft SQL Server 2005 with Service Pack 3 (SP3).

Listed below are the OS dependencies for the web servers and application servers in a farm:

- The 64-bit edition of Microsoft Windows 2008.
- The 64-bit edition of Microsoft Windows 2008 R2.

The SharePoint preparation tool installs a number of services and hot fixes prior to starting the product installation which update and prepare the Windows server environment, including the Web Server (IIS) role and the Application Server role.

The client computer accesses the SharePoint application by using a compatible browser such as Windows Internet Explorer.

2.3 Security Considerations

The SharePoint environment is an integrated platform rather than a single application. Thus, securing SharePoint must consider many areas and technologies. Security considerations may be categorized into the following general areas:

- Information flow planning prior to installation
- Server Protection at the OS level
- Communication Security from clients to the server environment
- Central Administration Site Security

- Collaboration Application Security
- Group (granular) permissions for securable objects
- Separation of roles and associated rights and privileges
- User Training tagging and metadata usage

3. SECURITY ASSESSMENT INFORMATION

The Microsoft® SharePoint Server Review targets conditions that undermine the integrity of security, contribute to inefficient security operations and administration, or may lead to interruption of production operations. The items reviewed are based on standards and practices published by Microsoft® (the vendor) and other security guidance entities, following guidance published in the Department of Defense Instruction (DoDI) 8500.2 and National Institute for Standards and Technology (NIST) Special Publication (SP) 800-53 security controls.

Defense Information Systems Agency (DISA) has assigned a level of urgency to each finding based on Chief Information Officer (CIO)-established criteria for Certification and Accreditation (C&A). All findings are based on regulations and guidelines. All findings require correction by the host organization.

3.1 SRR Review Method

To perform a successful SRR, this document provides the methods to assess vulnerabilities on Microsoft® SharePoint servers. In the initial release, all procedures are manual.

3.2 SRR Additional Considerations

To create these STIG requirements, the principles and guidelines found in the DoDI 8500.2 IA controls were applied to the SharePoint 2010 Server application. All collaboration applications used within DoD must adhere to these requirements. The SharePoint 2010 configuration tested was a basic default installation without third party or other enhancements. As a result, two new categories of items were defined.

Some requirements were determined to have been met natively by the application and cannot be configured or misconfigured during implementation. These requirements are marked as "permanent not a finding".

Some IA controls were not natively provided by the SharePoint default installation. These requirements are marked as a "permanent finding". Although, these requirements will not be a part of a SRR review, they represent residual risk to the DoD environment. Sites must take action to ensure these residual risks are mitigated or addressed either through use of network functionality, third party solutions, or documentation as appropriate.

Appendix A is an Excel spreadsheet which is provided as part of this STIG package. It contains a listing of all SharePoint requirements determined to be "permanent not a finding" and "permanent finding".