

UNCLASSIFIED



EMAIL SERVICES POLICY SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG) OVERVIEW

Version 2, Release 6

23 October 2015

Developed by DISA for the DoD

UNCLASSIFIED

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	2
1.4 STIG Distribution Email Services Policy STIG	2
1.5 Document Revisions	2
1.6 Other Considerations	2
2. REFERENCE DOCUMENTS	4

LIST OF TABLES

	Page
Table 1-1: Vulnerability Severity Category Code Definitions	2
Table 1-2: Reference Documents.....	4

1. INTRODUCTION

1.1 Executive Summary

This document is a requirement for all DoD-administered systems and all systems connected to DoD networks, as addressed in the technology section. These requirements are designed to assist System Managers (SMs), Information System Security Managers (ISSMs), Information System Security Officers (ISSOs), and System Administrators (SAs) with configuring and maintaining security controls.

Email systems are comprised of multiple products and services working together to enable transport and delivery of messages to users. This overview gives technology-specific background and information specific to the Email Services Policy.

The Email Services Policy Security Technical Implementation Guide (STIG), provides security policy and configuration requirements.

Policies that govern DoD installations are non-technical directives that must be part of every Exchange security review. Included are items such as performing regular conformance reviews, backups, and role-based assignment separation. Policies contribute to best practices for security in depth and continuity of operations.

Policies review is required for every email domain, regardless of the deployed email services product.

For an overview of all the Microsoft Exchange Server 2010 products and services, reference the Microsoft Exchange Server 2010 Server Security Technical Implementation Guide STIG Overview document at the following URL: <http://iase.disa.mil/stigs/app-security/app-servers/Pages/index.aspx>. The Microsoft Exchange Server 2010 Server Security Technical Implementation Guide STIG Overview also includes security review considerations to prepare for periodic assessments.

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 Email Services Policy STIG

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. REFERENCE DOCUMENTS

The following table enumerates the documents and resources referenced:

Table 2-2: Reference Documents

Date	Document Description	Source
2010	Microsoft Exchange Server 2010 Best Practices	Microsoft Press
January 2012	Microsoft Exchange Server 2010: Help	technet.microsoft.com
Current Version	Windows 2008 R2 STIG	iase.disa.mil
March 2012	Microsoft Exchange 2010 Security Guide	technet.microsoft.com
April 2013	SP 800 -53 Security and Privacy Controls in the Federal Information Systems and Organizations	http://csrc.nist.gov/publications/PubsSPs.html
February 2006	SP 800 -18 Guide for Developing Security Plans for Federal Information Systems	http://csrc.nist.gov/publications/PubsSPs.html