MICROSOFT EXCHANGE 2019
SECURITY TECHNICAL IMPLEMENTATION GUIDE
(STIG) OVERVIEW

30 January 2025

Developed by Microsoft and 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 the Defense Information Systems Agency (DISA) of any nonfederal entity, event, product, service, or enterprise.

TABLE OF CONTENTS

Page

LIST OF TABLES

Page

1. INTRODUCTION

1.1 Executive Summary

The Microsoft Exchange 2019 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 Windows Operating System (OS) STIG and any appropriate STIG(s) applicable to the system. This STIG comprises two parts:

- Microsoft Exchange 2019 Mailbox Server.
- Microsoft Exchange 2019 Edge Transport Server.

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 National Institute of Standards and Technology (NIST) Special Publication (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

Category	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.
- NIST Cryptographic Module Validation Program (CMVP) (https://csrc.nist.gov/groups/STM/cmvp/) IAW federal/DOD mandated standards.
- DODIN Approved Products List (APL) (https://aplits.disa.mil/processAPList.action) IAW DODI 8100.04.

2. ASSESSMENT CONSIDERATIONS

Email systems are composed of multiple products and services working together to enable transport and delivery of messages to users.

Edge Transport servers handle all inbound and outbound internet mail flow by providing mail relay and smart host services for the Exchange organization. Agents running on the Edge Transport server provide additional layers of message protection and security. These agents provide protection against spam and apply transport rules to control mail flow. All of these features work together to help minimize the exposure of the internal Exchange to threats on the internet.

The Edge Transport server role enables the organization to manage the following message-processing scenarios: internet mail flow, antispam protection, Edge Transport rules, and address rewriting.

The Mailbox Server role hosts mailboxes and advanced scheduling services for Microsoft Office Outlook and Microsoft Outlook Web App (OWA) users. It also performs processing and rendering for client connections proxied by the Client Access server and handles Unified Messaging requests. Mailbox servers may also host public folders, if desired. Overall, the Mailbox Server role provides a foundation for workflow, document sharing, and other forms of collaboration.

The Mailbox Server STIG must be reviewed on each Mailbox server in the Exchange environment.

The Email Domain Security Plan (EDSP) defines the security settings and other protections for email systems. It may be implemented as a standalone document or as a section within an umbrella System Security document, provided it contains the unique values engineered for that domain. Without a Security Plan, unqualified personnel may be assigned responsibilities they are incapable of meeting, and email security may become prone to an inconsistent or incomplete implementation. Because email systems are sufficiently unique, an EDSP is recommended.

For some email data categories, the product-specific STIG provides required security settings. For other categories, values can vary among domains, depending on the implementation and system sizing requirements. For example, tuning variables such as log sizes, mailbox quota limits, and partner domain security are engineered for optimal security and performance and should therefore be documented so reviews can assess whether they are set as intended. Assigned administrator names by role enable assessment of roles separation and least privilege permissions, as well as the ability to identify unauthorized access of processes or data. Backup and recovery artifacts, spam reputation providers, and antivirus vendors may differ by domain and will require operational support information to be recorded, such as license agreements, product copy locations, and storage requirements.

NIST SP 800-18, Guide for Developing Security Plans for Federal Information Systems, is publicly available and gives guidelines and a template for security plan creation. It can serve as a base for development if one is needed. At this writing, the document can be found at:
http://csrc.nist.gov/publications/PubsSPs.html.

Security controls applicable to email systems may not be tracked and followed if they are not identified in the EDSP. Omission of security control consideration could lead to an exploit of email system vulnerabilities or compromise of email information.