MICROSOFT ONENOTE 2013
SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG)
OVERVIEW

Version 1, Release 1

23 January 2015

Developed by DISA for the DoD

Trademark Information

TABLE OF CONTENTS

Page

LIST OF TABLES

Page

1. INTRODUCTION

This Microsoft Office Technology Overview, along with the associated Security Technical Implementation Guide (STIG), provides the technical security policies, requirements, and implementation details for applying security concepts to Commercial-Off-The-Shelf (COTS) applications.

The nearly universal presence of systems on the desktops of all levels of staff provides tremendous opportunities for office automation, communication, data sharing, and collaboration. Unfortunately, this presence also brings about dependence and vulnerabilities. Malicious and mischievous forces have attempted to take advantage of the vulnerabilities and dependencies to disrupt the work processes of the Government. Compounding this problem is the fact that the vendors of software applications have not expended sufficient effort to provide strong security in their applications. Where applications do offer security options, the default settings typically do not provide a strong security posture.

There are multiple STIG packages for Microsoft Office 2013, each contains technology-specific guidelines for the respective package. The Microsoft Office System 2013 must also be applied when any Office package is installed. The individual packages are:

- Microsoft Access 2013
- Microsoft Excel 2013
- Microsoft Groove 2013
- Microsoft InfoPath 2013
- Microsoft Lync 2013
- Microsoft Office System 2013
- Microsoft OneNote 2013
- Microsoft Outlook 2013
- Microsoft PowerPoint 2013
- Microsoft Project 2013
- Microsoft Publisher 2013
- Microsoft SharePoint Designer 2013
- Microsoft Visio 2013
- Microsoft Word 2013

This STIG contains security technical implementation guidance for Microsoft Office OneNote 2013 only.

1.1 Executive Summary

This document is a requirement for all DoD administered systems and all systems connected to DoD networks. These requirements are designed to assist Security Managers (SMs), Information Assurance Managers (IAMs), Information Assurance Officers (IAOs), and System Administrators (SAs) with configuring and maintaining security controls. This guidance

supports DoD system design, development, implementation, certification, and accreditation efforts.

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 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.letterkenny.FSO.mbx.stig-customer-support-mailbox@mail.mil. DISA Field Security Operations (FSO) will coordinate all change requests with the relevant DoD organizations before inclusion in this document.