

UNCLASSIFIED



# **MICROSOFT OFFICE ONENOTE 2010 SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG) OVERVIEW**

Version 1, Release 1

23 JANUARY 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 FSO of any non-Federal entity, event, product, service, or enterprise.

**TABLE OF CONTENTS**

	<b>Page</b>
<b>1. INTRODUCTION.....</b>	<b>1</b>
1.1 Executive Summary .....	1
1.2 Authority .....	2
1.3 Vulnerability Severity Category Code Definitions .....	2
1.4 STIG Distribution.....	2
1.5 Document Revisions .....	3

**LIST OF TABLES**

	<b>Page</b>
Table 1-1: Vulnerability Severity Category Code Definitions .....	2

## 1. INTRODUCTION

### 1.1 Executive Summary

This Microsoft Office OneNote 2010 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.

The requirements and recommendations set forth in this document will assist Information Assurance Officers (ISSO) and Information Assurance Managers (ISSMs) in protecting desktop applications in DoD locations hereafter referred to as sites. The responsible Configuration Control Board (CCB) will approve revisions to site systems that could have a security impact. Therefore, before implementing desktop application security measures, the ISSO will submit a change notice to the CCB for review and approval.

Although there are a few different operating system platforms for desktop environments, the security requirements detailed in this document target to applications installed on Microsoft Windows 7 platforms only.

This STIG contains security technical implementation guidance for Microsoft Office OneNote 2010 only.

There are multiple STIG packages for Microsoft Office 2010; each contains technology-specific guidelines for the respective package that are to be applied along with the Microsoft Office System guidelines. The individual packages are:

- Microsoft Access 2010
- Microsoft Excel 2010
- Microsoft InfoPath 2010
- Microsoft Office System 2010
- Microsoft OneNote 2010
- Microsoft Outlook 2010
- Microsoft PowerPoint 2010
- Microsoft Project 2010
- Microsoft Publisher 2010
- Microsoft Word 2010

## 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, <b>directly and immediately</b> result in loss of Confidentiality, Availability, or Integrity.
CAT II	Any vulnerability, the exploitation of which <b>has a potential</b> to result in loss of Confidentiality, Availability, or Integrity.
CAT III	Any vulnerability, the existence of which <b>degrades measures</b> 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](mailto: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. Approved changes will be made in accordance with the DISA FSO maintenance release schedule.