MICROSOFT OFFICE 2010 SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG) OVERVIEW

Version 1, Release 12

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

This Microsoft Office 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 System Security Officers (ISSOs) and Information System Security 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.

There are multiple STIG packages for Microsoft Office 2010, each contains technology-specific guidelines for the respective package along with the overall Microsoft Office System requirements. The individual packages are:

- Microsoft Access 2010
- Microsoft Excel 2010
- Microsoft InfoPath 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 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. SECURITY ASSESSMENT INFORMATION

2.1 Manual Review

To conduct a manual review of compliance with the Microsoft Office STIG requirements, it is necessary to use some tools that are provided with the Windows operating system. Some of these tools are as follows:

- Windows Explorer
- Windows "Edit File Type" facility – accessed through the Windows Explorer Windows Registry Editor – regedit.exe or regedt32.exe
- Windows Search – accessed via the Windows Start Menu Group Policy Object Editor – gpedit.msc
- Microsoft Management Console (MMC)
- Microsoft Security Configuration and Analysis snap-in (used with the MMC)

Registry paths and values identified in each control assume the use of Group Policy Object Editor in the Microsoft Management Console, with installation of Microsoft Office 2010 Administrative Templates. Installations not using Group Policies to administer Microsoft Office products may observe alternate registry paths for stored configuration values. For example, registry keys for Internet Explorer settings are listed in the STIG as HKLM\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ADDON_MANAGEMENT but may appear under HKLM\Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ADDON_MANAGEMENT.

Instructions for the manual remediation of vulnerabilities, to include adding, deleting, and modifying settings can be found in the "Fix" information provided in the VMS vulnerability.

It must be noted that the guidelines specified should be evaluated in a local, representative test environment before implementation within large user populations. The extensive variety of environments makes it impossible to test these guidelines for all potential software configurations. For some environments, failure to test before implementation may lead to a loss of required functionality.

2.2 Software Maintenance

Maintaining the security of office automation products requires frequent reviews of security bulletins. Many security bulletins mandate the installation of a software patch to overcome security vulnerabilities.

SAs and ISSOs should regularly check vendor web sites for information on new security patches that are applicable to their sites. All applicable security patches will be applied to the system. A security patch is deemed applicable if the product is installed, even if it is not used or is disabled.

FSO does not test or approve patches or service packs. It is the site's responsibility to test vendor patches within its test environment.

SAs and ISSOs should regularly check office automation product vendor web sites for information concerning products or versions of products no longer being supported. Action should be taken to ensure a smooth migration plan is developed and implemented prior to a product going into a non-support status.