MICROSOFT OFFICE 2013 SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG) OVERVIEW

Version 1, Release 5

24 July 2015

Developed by 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 DISA or any non-Federal entity, event, product, service, or enterprise.

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 and should be applied along with the Microsoft Office System 2013 STIG requirements. 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

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 System Security Managers (ISSMs), Information System Security Officers (ISSOs), 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 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. ASSESSMENT CONSIDERATIONS

This document is based on Microsoft Office 2013 installations within the Windows 7 Operating System and the Windows 8 Operating System. This document, and associated STIGs, has set forth requirements based upon having a secured Windows environment. The superset of these requirements can be found in the appropriate Windows STIG, which is also available from the IASE website. Failure to apply these requirements will significantly diminish the value of the specifications in this document, as well as diminish the overall security posture of the asset to which these settings apply.

Security controls applied to the underlying operating system platform will directly affect the strength of the security that surrounds desktop applications.

The security requirements detailed in this document target applications installed on Microsoft Windows 7/Windows 8 platforms only, using the traditional Windows Installer-based (MSI) method of installing and updating Office.

2.1 Security Assessment Information

2.1.1 Microsoft Office Technology

2.1.1.1 Office 2013 Additional Technology

Office 2013 introduced additional technologies including the ability to use/update the cloud, touch capabilities, and a more streamlined, ribbon-less interface in the products making up the suite. Specific settings have been included to ensure disabling of saving to the cloud.

Additional Office 2013 functionality introduced extended settings, some of which were not deemed to impact the security posture of the system. Under those circumstances, specific STIG requirements were not developed.

Other Office 2013 extended settings were determined to affect the security posture of the system and have been included as additional STIG requirement settings.

Also introduced in this Office STIG version are individual STIGs for the Visio 2013, Lync (client) 2013, SharePoint Design 2013, and OneDrive Pro (formerly SkyDrive Pro) (Groove) 2013 products.

2.1.1.2 OneDrive (formerly SkyDrive) vs. OneDrive Pro (formerly SkyDrive Pro)

It is notable to differentiate between OneDrive and OneDrive Pro (Groove). OneDrive is Microsoft's consumer cloud storage solution. OneDrive Pro, however, is aimed at corporate users and provides much of the same experience that OneDrive (cloud) provides to consumer users, but adds the ability for a corporate IT department to define security/search/content policies. OneDrive is a personal cloud storage capability for an individual's personal files,

managed by the individual, using the public cloud, and is currently not allowed from a DoD network. OneDrive Pro is site's cloud storage for work documents, managed by local IT personnel and uses local SharePoint or on-premises storage. The guidance provided in the Groove 2013 is for the purposes of OneDrive Pro (groove.exe) and does not relate to the OneDrive commercial cloud use.

2.1.1.3 Office 365

Office 365 is a subscription-based online office suite, providing hosted email and Microsoft Office 2013 desktop applications (WebApps). It is installed via the Click-to-Run installation option. Office 365 is not deployed or used in the DoD and this STIG does not cover any setting related to the Office 365 online suite.

2.1.1.4 Click-to-Run

Click-to-Run is a Microsoft streaming and virtualization technology that is also used to install and update Microsoft Office 2013 desktop products, as an alternative to the traditional Windows Installer-based (MSI) method. These streaming and virtualization capabilities are based on technologies in Microsoft Application Virtualization (App-V). In Office 2010, Click-to-Run was available to only consumer users. In this new release, Click-to-Run supports large enterprise deployments. Guidance for Click-to-Run installations is not provided in this STIG.

Although not specifically included in this STIG, Office 365 and Click-to-Run technologies may be referenced in STIG requirements and vulnerability discussions.

2.1.2 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 2013 Administrative Templates. Installations not using Group Policies to administer Microsoft Office products may observe alternate registry paths for stored configuration values. 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.

If only one application of the Microsoft Office suite is installed (i.e., Microsoft Office Word only or Microsoft Office Excel only), the Microsoft Office System STIG settings must also be applied, along with the STIG settings for the installed application. The Microsoft Office System STIG is included in each of the individual application STIG packages in addition to being included as a separate STIG.

2.1.3 Other Considerations

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.

It is especially important to fully test with specific and legacy applications which is dependent upon the Microsoft Office applications for functionality, as well as Microsoft Office Add-ins which are currently used in the environment.

3. CONCEPTS AND TERMINOLOGY CONVENTIONS

3.1 Terminology Conventions

Current desktop applications present a graphical user interface (GUI) for their use and parameter customization. Most of the parameter settings specified in this document can be examined and changed through the application's GUI, subject to Windows policy settings. The following terms are used in describing how to view or configure the settings:

- Dialog – An application dialog is a window presented by the application.
- Menu – An application menu consists of a textual list of actions, commands, or (sometimes) options that can be selected.
- Enable – The term enable is used to describe the selection of a parameter setting, often indicated as an option button or check box in the application GUI. For example, when a parameter setting specifies "enable", the associated option button display would indicate that the option is selected.

  NOTE: Many Microsoft settings actually disable a specific function of the application. By selecting to "Enable" those settings, the net effect is to disable the specified function.

- Disable – The term disable is used to describe the de-selection of a parameter setting, often indicated as an option button or check box in the application GUI. For example, when a parameter setting specifies "disable", the associated option button display would indicate that the option is de-selected.

  NOTE: Some Microsoft settings enable a specific function of the application. By selecting to "Disable" those settings, the net effect is to enable the specified function.

  - When evaluating the Enable and Disable settings, it is important to understand the underlying STIG requirement.

- Check box – The term check box is used to describe a setting which can be specifically selected, or not. If selected, the value it represents will be applied. If not selected, the value of the setting will not be applied.

3.2 Writing Conventions

Throughout this document, statements are written using words such as "**must**" and "**must be**".

A reference that uses "**must**" indicates mandatory compliance. The ISSO will adhere to the instruction as written.

When the reference indicates a **"must"** or **"must be"** directive, the check verbiage typically will indicate a "Verify the policy value" "is set to" pairing which, when verified and applied, will result in meeting the **"must"** or **"must be"** directive.

- A "Not a Finding" statement will be indicated for when the **"must"** or **"must be"** directive has been met. It is implied that any other setting, including the absence of a setting, would be deemed as an "Open Finding".

3.3 Security Best Practices/Standardization

STIG setting requirements are based upon known vulnerabilities, or the likelihood of vulnerabilities, associated with a specific functionality.

There are, however, some functions of an application which warrant the strict adherence to standardization in order to facilitate a secure operating environment, even when the setting is not specifically applicable to a known or perceived vulnerability.

As a result, some STIG settings have been deemed as a requirement in order to establish that standardization within a DoD site's environment.

Example:

Opening Microsoft Office legacy-formatted files could introduce malicious code. Prohibiting the opening of these legacy-formatted files is generally accepted as a necessity to protect the security posture of the system and local network.

The ability to save a Microsoft Office document in one of those legacy or foreign formats is not seemingly associated with known or perceived vulnerabilities. But if the saving of those formats were allowed, while the opening of those formats is prohibited, users would not be able to access the files they have saved.

By requiring the "Save-as" functionality be compatible with the "Open-as" functionality, standardization on the network will be achieved while also ensuring user accessibility to those saved files.

APPENDIX A: Related Publications

Government Publications

NIST Special Publication 800-53 Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations* (Final)

NIST Special Publication 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems* (Final)

NIST Special Publication 800-53A, Revision 1, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans* (Final)

Department of Defense, DoD Directive (DoDD) 8500.1, "Information Assurance (IA)," October 24, 2002.

Department of Defense, DoD Instruction (DoDI) 8500.2, "Information Assurance (IA)," February 6, 2003.

Department of Defense, DoD Directive (DoDD) 8552.01, "Use of Mobile Code Technologies in Department of Defense (DoD) Information Systems," 23 October 2006.

Department of Defense Instruction, "Department of Defense (DoD) Public Key Infrastructure (PKI) and Public Key (PK) Enabling", 24 May 2011.

Department of Defense, "X.509 Certificate Policy for the United States Department of Defense," Version 5.2, 13 November 2000.

Defense Information Systems Agency, "Secure Remote Computing STIG", Current Version.

Executive Office of the President, Office of Management and Budget Memorandum, "Protection of Sensitive Agency Information", 23 June 2006.

National Security Agency (NSA), "E-mail Security in the Wake of Recent Malicious Code Incidents," Version 2.6, 29 January 2002.

National Security Agency (NSA), "Microsoft Office 2000 Executable Content Security Risks and Countermeasures," 8 February 2002.

National Security Agency (NSA), "Microsoft Office XP/2003 Executable Content Security Risks and Countermeasures," 10 February 2005.

APPENDIX B: Related Websites

Government Web Sites

http://www.nist.gov/itl/csd/soi/fisma.cfm NIST FISMA Implementation Project
http://www.disa.mil/ Defense Information Systems Agency
http://iase.disa.mil/ (NIPRNet)
Defense Information Systems Agency Information Assurance Support Environment
https://www.cybercom.mil (NIPRNet) United States Cyber Command (USCYBERCOM)
https://patches.csd.disa.mil DoD Patch Repository
http://dodpki.c3pki.chamb.disa.mil/ or http://dodpki.c3pki.den.disa.mil/
Department of Defense Class 3 Public Key Infrastructure (PKI) Home Page

Commercial and Other Non-government Sites

http://www.icsalabs.com/ International Computer Security Association (ICSA) Labs
http://www.mozilla.org FireFox Information
http://www.mcafee.com/support/ McAfee Support
http://www.microsoft.com/download/en/default.aspx Microsoft Download Center
http://windows.microsoft.com/en-US/internet-explorer/products/ie/home
Microsoft IE Product Downloads
http://technet.microsoft.com/en-us/security Microsoft TechNet Security
http://www.symantec.com/techsupp/ Symantec Service & Support
http://technet.microsoft.com/en-us/library/cc179178.aspx
Microsoft What's new in Office 2013
http://technet.microsoft.com/en-us/library/cc303401.aspx
Microsoft Office 2013 Resource Kit
http://technet.microsoft.com/en-us/library/cc178992.aspx
Group Policy Administrative Template files for Office 2013