MICROSOFT OFFICE 2016
SECURITY TECHNICAL IMPLEMENTATION GUIDES (STIGs) OVERVIEW

Version 1, Release 2

19 January 2017

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

TABLE OF CONTENTS

Page

1. INTRODUCTION 1

1.1 Executive Summary 1
1.2 Authority 1
1.3 Vulnerability Severity Category Code Definitions 2
1.4 STIG Distribution 2
1.5 SRG Compliance Reporting 2
1.6 Document Revisions 2
1.7 Other Considerations 2
1.8 Product Approval Disclaimer 3

2. ASSESSMENT CONSIDERATIONS 4

2.1 Product Updates for Office 2016 4
2.2 OneDrive vs. OneDrive for Business 4
2.3 Manual Review 4
2.4 Other Considerations 5

LIST OF TABLES

Page

Table 1-1: Vulnerability Severity Category Code Definitions 2

1. INTRODUCTION

1.1 Executive Summary

The Microsoft Office 2016 Security Technical Implementation Guides (STIGs) provide the technical security policies, requirements, and implementation details for applying security concepts to Office 2016 applications. These documents are meant to improve the security of Department of Defense (DoD) information systems.

There are multiple STIG packages for Microsoft Office 2016, each contains technology-specific guidelines for the respective package. The Microsoft Office System 2016 STIG must also be applied when any Office 2016 package is installed. The individual packages are:

- Microsoft Access 2016
- Microsoft Excel 2016
- Microsoft Office System 2016
- Microsoft OneDrive for Business 2016
- Microsoft OneNote 2016
- Microsoft Outlook 2016
- Microsoft PowerPoint 2016
- Microsoft Project 2016
- Microsoft Publisher 2016
- Microsoft Skype for Business 2016
- Microsoft Visio 2016
- Microsoft Word 2016

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 SRG Compliance Reporting

All technical NIST SP 800-53 requirements were considered while developing these STIGs. Requirements that are applicable and configurable will be included in the final STIG. A report marked For Official Use Only (FOUO) will be available for those 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 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.

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). DoD Authorizing Officials (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 vendor's proprietary information.

AOs have the purview to determine product use/approval 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) (http://www.niap-ccevs.org/) IAW CNSSP #11
- National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) (http://csrc.nist.gov/groups/STM/cmvp/) IAW Federal/DoD mandated standards
- DoD Unified Capabilities (UC) Approved Products List (APL) (http://www.disa.mil/network-services/ucco) IAW DoDI 8100.04

2. ASSESSMENT CONSIDERATIONS

This document is based on Microsoft Office 2016 installations within the Windows 10 Operating System. This document, and associated STIG, 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 10 platform only, using the traditional Windows Installer-based (MSI) method of installing and updating Office.

2.1 Product Updates for Office 2016

Office 2016 has removed several applications from the product suite. InfoPath and SharePoint Designer are no longer part of the suite. Lync has been renamed to Skype for Business. Groove has been renamed to OneDrive for Business.

2.2 OneDrive vs. OneDrive for Business

It is notable to differentiate between OneDrive and OneDrive for Business (ODfB). OneDrive is Microsoft's consumer cloud storage solution. ODfB, however, is aimed at corporate users and provides much of the same experience that OneDrive does, 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. ODfB is a 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 OneDrive for Business 2016 STIG is for the purposes of ODfB and does not relate to the commercial OneDrive.

2.3 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 Registry Editor – regedit.exe or regedt32.exe
- 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 2016 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.

The policy path will be slightly different depending on what tool is being used to check/generate the policy. If using the Group Policy Management console on a domain controller, the path is "Computer/User Configuration -> Policies -> Administrative Templates -> <path>." If using gpedit.msc on a non-DC system, the path is "Computer/User Configuration -> Administrative Templates -> <path>."

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.

There are no Group Policy Objects (GPOs) for the legacy OneDrive client however the new client (OneDrive for Business) does contain GPO support and was added. The templates can be found at this link. (https://www.microsoft.com/en-us/download/details.aspx?id=50381)

2.4 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.