APPLE OS X 10.11 (EL CAPITAN) SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG) OVERVIEW

Version 1, Release 2

28 October 2016

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

LIST OF TABLES

Page

1. INTRODUCTION

1.1 Executive Summary

The Apple OS X 10.11 Security Technical Implementation Guide (STIG) provides security policy and configuration requirements for the use of Apple OS X 10.11 in the Department of Defense (DoD). Guidance in these documents applies only to Apple OS X 10.11 and related components on DoD systems and excludes any other components or software running on DoD systems. Hardening the Apple OS X Server application suite is not addressed in these documents.

The Apple OS X 10.11 STIG presumes operation in an environment compliant with all applicable DoD guidance, especially concerning remote access and network infrastructure.

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 provides 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 this STIG. 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 configuration 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 percent 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 the 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

2.1 Security Assessment Information

This section should be reviewed by DoD personnel or contractors either preparing for or conducting Apple OS X security assessments. To perform an assessment, a reviewer will need access to the Apple OS X Configuration Profiles, the Apple OS X systems subject to the review, and in many cases, a centralized management tool.

Multiple Configuration Profiles can be deployed to the Apple OS X system. The reviewer must be aware that the compliant setting may be found in any one of them, and they will need to work with the Apple OS X system administrator to determine which Configuration Profiles are relevant to the review. See Section 3.1 below for information on how Configuration Profiles work and how they are distributed.

The reviewer will need to select a tool for viewing the Configuration Profiles. Typically, this will be the same tool that the Apple OS X system administrator uses to distribute the Configuration Profiles. The reviewer may also examine each Configuration Profile directly using a text editor.

Compliance verification involves both the Configuration Profile and the configuration on the Apple OS X system. Checking the Configuration Profile ensures that it contains the correct content. Checking the Apple OS X system ensures that the Configuration Profile has been installed on the device or that the desired behavior resulting from the configuration is present.

3. CONCEPTS AND TERMINOLOGY CONVENTIONS

This section outlines best practices and recommendations for Apple OS X 10.11.

3.1 Configuration Profiles

A Configuration Profile is an XML file that applies configuration information to an Apple OS X system. Administrators should use a Configuration Profile for each IA control category (e.g., Passcode Policy, Restrictions, Login Window, etc.), rather than a single profile containing all potential settings. The use of multiple profiles allows for flexible updates without affecting standard configurations.

If the same configuration is set in multiple profiles on a device, the most restrictive settings take precedence. For example, if one profile sets a passcode length requirement of six characters and another profile sets a passcode length requirement of seven complex characters, the user will be required to set a passcode of seven complex characters. In other words, it will enforce the combination of the more restrictive length setting from one profile and the more restrictive character requirement from the other profile.

Settings that are defined by an installed Configuration Profile cannot be changed by the user. In some cases, a user can opt to make a setting more restrictive than what is defined in the profile. For example, if a Configuration Profile requires the device to lock after 15 minutes, the user can set the device to lock immediately. If the user deletes a Configuration Profile, all the settings defined by the profile are removed.

Several Configuration Profiles are included with the STIG:

- Apple OS X 10.11 STIG Restrictions Policy (used to apply generic restrictions)
- Apple OS X 10.11 STIG Passcode Policy (used to enforce password requirements)
- Apple OS X 10.11 STIG Security and Privacy Policy (used to enforce requirements relating to security and privacy)
- Apple OS X 10.11 STIG Login Window Policy (used to enforce login window requirements)
- Apple OS X 10.11 STIG Bluetooth Policy (used to disable Bluetooth)
- Apple OS X 10.11 STIG Application Restrictions Policy (used to disable applications with iCloud connections)
- Apple OS X 10.11 STIG Disable iCloud Policy (used to disable iCloud)
- Apple OS X 10.11 STIG Custom Policy (used to apply other requirements)

These Configuration Profiles include settings for STIG requirements indicated as being set in a configuration profile.

Organizations that use these Configuration Profiles should first import them into the Apple OS X management tool of their choice and sign them to ensure integrity and non-repudiation of source. The signed profiles can then be deployed as appropriate.

3.2 Deploying Configuration Profiles

There are several ways to deploy Configuration Profiles depending on the use case, quantity of Apple OS X systems, and workflow. Refer to the Apple Technical White Paper “Managing OS X with Configuration Profiles” for more information.

3.3 Apple ID

An Apple ID is a user’s username for the iTunes Store, App Store, iCloud, and other Apple services. In the DoD, an Apple ID is needed on an Apple OS X system for two purposes:

- Downloading and updating App Store apps and Apple OS X maintenance content
- Downloading content from the iTunes Store

The use of Apple IDs does not pose a significant IA risk when applications containing DoD-sensitive information are managed appropriately. Apple IDs are not designed to be managed by an organization, and no tools are provided to accomplish such administration. DoD organizations should avoid issuing organizationally generated Apple IDs, including custom email addresses just for the purpose of Apple OS X system administration.

To obtain an Apple ID, the user must agree to Apple's Terms and Conditions. DoD cannot serve as a proxy for a user’s acceptance of the Terms and Conditions. Users can create an Apple ID on the Apple OS X system or online at https://appleid.apple.com. An Apple knowledge base article at http://support.apple.com/kb/HT2534 explains how to create an Apple ID without a credit card. It is recommended that each user use his or her primary DoD email address for the Apple ID. However, it is acceptable to use a previously created personal Apple ID on government-furnished Apple OS X systems, provided that this ID is not a member of a Family Sharing group.

Apple IDs are protected by passcodes to prevent unauthorized use. The Apple ID passcodes are distinct from the Apple OS X system unlock passcode. Organizations have no technical means to reset passcodes or enforce password complexity rules on Apple ID passcodes. Users should be encouraged to select Apple ID passcodes within DoD guidelines. For example, the following rules should be used:

- Be at least 15 characters long
- Contain at least one upper-case alphabetic character
- Have at least one lower-case alphabetic character
- Have at least one numeric character
- Have at least one special character (e.g. ~ ! @ # $ % ^ & * ( ) _ + = - ' [ ] / ? > <)

Apple sends clear text messages containing the name of the Apple OS X system to the Apple ID email address. For this reason, Apple OS X system names should not reveal a DoD affiliation, PII, or other sensitive information.

3.4 Apps

This section will discuss the Apple App Store and applications bundled with Apple OS X. Disabled apps should be evaluated against mission needs and should only be allowed if approved by the AO.

3.4.1 Apple App Store

The App Store is an application distribution platform for commercially available Apple OS X apps. Apps in the App Store are reviewed by Apple and digitally signed for use on Apple OS X systems. The App Store application on the Apple OS X system must be enabled to install and update commercially available apps, even if the organization's preferred method is to obtain apps through other means. To avoid installing unauthorized apps, users should be discouraged from obtaining apps directly from the App Store. Not all of the applications in the App Store are appropriate for use on Government-Furnished Equipment (GFE). DoD organizations must establish their own app vetting and approval processes to determine which applications are appropriate for their use cases.

Applications purchased with an Apple ID are available to other Apple OS X systems configured with the same Apple ID. Previously purchased applications will not automatically download on a new device when an existing Apple ID is first associated with it. Users should be discouraged from subsequently synchronizing applications across personally owned and government-furnished Apple OS X systems. To prevent applications acquired for personal use from automatically downloading on a government-furnished Apple OS X system, the user should turn off "Automatically download apps purchased on other Macs" from the App Store setting pane in System Preferences.

3.4.2 iTunes

The iTunes app, configured in accordance with the STIG, is allowed in the DoD.

3.4.3 Safari

The Safari app is allowed for use in the DoD, to include using with a CAC for handling FOUO information.

3.4.4 Mail

The Mail application is disabled, per the STIG. It is not compatible with DoD email systems. This app is disabled due to connectivity to iCloud, which cannot be adequately controlled.

3.4.5 Calendar

The Contacts app is disabled, per the STIG. This app is disabled due to connectivity to iCloud, which cannot be adequately controlled.

3.4.6 Contacts

The Contacts app is disabled, per the STIG. This app is disabled due to connectivity to iCloud, which cannot be adequately controlled.

3.4.7 Reminders

The Reminders app is disabled, per the STIG. This app is disabled due to connectivity to iCloud, which cannot be adequately controlled.

3.4.8 Messages

The Messages app is disabled, per the STIG. This app is disabled due to connectivity to iCloud, which cannot be adequately controlled.

3.4.9 Notes

The Notes app is disabled, per the STIG. This app is disabled due to connectivity to iCloud, which cannot be adequately controlled.

3.4.10 FaceTime

The FaceTime app is disabled, per the STIG. This app is disabled due to connectivity to iCloud, which cannot be adequately controlled.

3.4.11 Game Center

The Game Center app is disabled, per the STIG. This app is disabled due to connectivity to iCloud, which cannot be adequately controlled.

3.5 AirDrop

The AirDrop service is disabled, per the STIG, and is not approved for use in the DoD.

3.6 AirPlay

AirPlay allows a user to wirelessly stream content from his or her Apple OS X system to hardware that supports the AirPlay protocol, such as Apple TV. The contents of AirPlay streams are protected by multiple security protocols. To ensure users only send content to the intended Apple TV, the Apple TV should be configured to use an onscreen code. Users will need to enter the code each time they would like to transmit from their Apple OS X systems to the Apple TV.

3.7 Apple Push Notification Service

Apple Push Notification Service (APNS) is an encrypted and authenticated communication tool allowed for use in the DoD.

3.8 iCloud

At this time, the Apple iCloud service does not have FedRAMP certification. Its use in the DoD is not authorized on Apple OS X systems.

4. GENERAL SECURITY REQUIREMENTS

This section outlines security-relevant information for Apple OS X 10.11.

4.1 Federal Information Processing Standard (FIPS) 140-2

The cryptographic modules supporting Apple OS X 10.11 have not been FIPS 140-2 validated as of the date of this publication but are in process. DoD organizations using Apple OS X 10.11 should visit the following website to obtain updates on validation status:

http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401vend.htm

The cryptographic modules supporting Apple OS X 10.10 are being revalidated to accommodate new features in Apple OS X 10.11. The previously validated cryptographic modules are:

- CoreCrypto Module v5.0, which supports applications and services such as S/MIME and HTTPS
- CoreCrypto Kernel Module v5.0, which is used by the kernel for low-level OS X functions, such as secure boot validation and protection of data at rest (DAR)

4.2 Software Updates

Keeping Apple OS X up to date ensures that it has the latest enhancements and security controls in place. This STIG requires that all updates come from an approved source. Apple is considered a DoD-approved source. Apple-provided updates can be installed on Apple OS X systems when available, with the exception that users should not install the next major release until authorized to do so. This STIG assumes that the latest version of Apple OS X 10.11 is installed.

4.3 Common Access Card (CAC)

CACs include embedded private keys to perform a number of functions, such as digitally signing email, decrypting email, authenticating to DoD public key-enabled websites, and authenticating to VPN concentrators. In Apple OS X, hard token (smart card) transactions are handled by third-party applications. To fulfill the functions performed with CACs, there are a variety of applications that have CAC support (for example: DoD PKI-enabled web browser, S/MIME email client, and VPN). CAC readers are available for Apple OS X systems.