APPLE iOS 11
SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG) OVERVIEW

Version 1, Release 1

11 December 2017

Developed by Apple and DISA for the DoD

Trademark Information

TABLE OF CONTENTS

Page

LIST OF TABLES

Page

1. INTRODUCTION

1.1 Executive Summary

The Apple iOS 11 Security Technical Implementation Guide (STIG) provides the technical security policies, requirements, and implementation details for applying security concepts to Apple devices running iOS 11 that process, store, or transmit unclassified data marked as "Controlled Unclassified Information (CUI)" or below. The STIG is based on the Protection Profile for Mobile Device Fundamentals (MDFPP) version 3.1 STIG Template. Requirements compliance is achieved by leveraging a combination of configuration profiles, user-based enforcement (UBE), and reporting. DoD Common Access Card (CAC) and the DoD Information System Consent Banner can be supported with third-party software.

The scope of this STIG covers only the Corporate Owned Personally Enabled (COPE) and Corporate Owned Business Only (COBO)[1] use cases. The Bring Your Own Device (BYOD) and Choose Your Own Device (CYOD)[2] use cases are not in scope for this STIG. The office of the DoD Chief Information Officer (CIO) is developing a DoD way forward and business case for BYOD, and the BYOD and/or CYOD use cases may be included in a future version of the STIG.

This STIG assumes that for the COPE use case, the technology used for data separation between work apps and data and personal apps and data has been certified by the National Information Assurance Partnership (NIAP) as compliant with the data separation requirements of the Protection Profile for Mobile Device Fundamentals (MDF)[3]. As of the publication date of this STIG, the only data separation technology or application that is NIAP-certified for an Apple iOS device is the native iOS managed – unmanaged application technology. Please see Section 3.5, "Apps", in the STIG Supplemental document for more information.

The configuration requirements and controls implemented by this STIG allow unrestricted activity by the user in downloading and installing personal (unmanaged) apps and data (music, photos, etc.) with Authorizing Official (AO) approval and within any restrictions imposed by the AO. See the STIG Supplemental document, Section 2.10, "Configuration of Unmanaged Apps", for more information.

Note: If the AO has approved the use/storage of DoD data in one or more personal (unmanaged) apps, allowing unrestricted activity by the user in downloading and installing personal (unmanaged) apps on the iOS 11 device may not be warranted due to the risk of possible loss of or unauthorized access to DoD data.

This STIG assumes that if a DoD WiFi network allows an iOS mobile device to connect to the network, the WiFi network complies with the Network Infrastructure STIG; for example, wireless access points and bridges must not be directly connected to the enclave network.

[1] Work data/apps only – no personal data/apps
[2] Similar to BYOD but only select models of personal devices are allowed.
[3] The primary Protection Profile requirement is FDP_ACF_EXT.1.2.

Supervision of iOS devices was introduced by Apple with iOS 5 and provides the administrator more control of an iOS device than is available for an unsupervised device. Supervised mode is intended for institutionally owned devices. Supervised mode provides the DoD more control over managed iOS devices by providing access to additional device management controls, including disabling a user from modifying installed accounts, removing the management profile (MDM profile), or accessing the Apple App Store. The DoD expects Apple to move one or more critical security controls, including iCloud backup, from unsupervised to supervised mode in the near future. Supervised mode is not a current DoD requirement but is considered an industry best practice for Government-owned devices to be supervised.

An MDM can only implement supervised profile elements on iOS devices that are supervised. A device can be supervised using one of two methods: First, it can be enrolled in Apple's Device Enrollment Program (DEP) and supervised during the activation of the device. Second, an iOS device can be placed in supervised mode by using the Apple Configurator (AC2) tool. DEP registration of an iOS device can occur if an iOS device is purchased directly from Apple (Apple Government Team or Apple's Retail Business team), an Apple authorized reseller, or manually via AC2. The DoD procurement office will need to provide the third-party reseller with the agency's DEP customer number, which can be obtained by applying at http://deploy.apple.com as a business.

DISA recommends DoD procurement offices immediately institute a procurement process in which all iOS device procurements require that the device be enrolled in DEP. In addition, current iOS device inventory should be registered in DEP through the reseller the devices were purchased from, and any device not eligible for enrollment in DEP should be identified as soon as possible. Devices not able to be enrolled in DEP can still be supervised and added to the agency's DEP account with AC2.

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 MDFPP Compliance Reporting

All Protection Profile for Mobile Device Fundamentals and DoD Annex security functional requirements (SFRs) were considered while developing this STIG. In DoD environments, devices must implement SFRs as specified in the DoD Annex to the MDFPP.

Requirements that are applicable and configurable are included in this STIG.

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