APPLE iOS 11
SUPPLEMENTAL PROCEDURES

Version 1, Release 1

11 December 2017

Developed by Apple and 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

1. SECURITY READINESS REVIEW

1.1 General

When conducting an Apple iOS Security Readiness Review (SRR), the Team Lead and the assigned Reviewer identify security deficiencies and provide data from which to predict the effectiveness of proposed or implemented security measures associated with Apple iOS and its associated Mobile Device Management (MDM) software or other centralized management solution.

1.2 Mobile Policy Review

Detailed policy guidance is available on the DISA Information Assurance Support Environment (IASE) website at: http://iase.disa.mil/stigs/mobility/Pages/policies.aspx

Use the Mobility Policy Security Technical Implementation Guide (STIG) and the CMD Policy STIG to review the Smartphone Handheld asset.

2. MOBILE DEVICE PROCEDURES

2.1 Apple iOS Wipe Procedures

A security wipe is designed to permanently delete data so it cannot be recovered. This includes email accounts, downloaded apps, media files, documents, browser bookmarks, and settings. These procedures are appropriate for iOS 11 devices never exposed to classified data.

2.2 Wipe on Device

When the device is being reprovisioned for a new user, the user or administrator should implement the on-device wipe procedure.

To wipe the device, perform the following steps:

1. Open the Settings app.
2. Tap “General”.
3. Tap “Reset”.
4. Tap “Erase All Content and Settings”.
5. Enter the device unlock passcode.

2.3 Activation Lock

To disable Activation Lock, perform the following steps on an unlocked Apple iOS device:

1. Open the Settings app.
2. Tap “iCloud”.
3. Turn off “Find My iPhone” by moving the switch to the left so it no longer appears green.
4. Enter the password for the specified Apple ID in the text box provided for this purpose.
5. Tap on “Turn Off”.

2.4 Wipe from MDM Console

If the wipe is being performed as part of a reprovisioning process, the user or administrator should disable Activation Lock using the steps listed above. The steps for wiping an Apple iOS device from an MDM console will vary depending on the MDM software used. As an example, on the MobileIron Admin Portal, perform the following steps:

1. Select the “USERS AND DEVICES” tab.
2. Select the device to be wiped.
3. Select “Actions” on the menu bar.
4. Select “Wipe” from the drop-down menu.
5. Click or tap the “Wipe” button in the dialog box to confirm the wipe command.

The Apple iOS wipe function resets the device to factory defaults. Without the key to decrypt previously stored data, it is essentially inaccessible to any subsequent user. The key is derived

from the user's device unlock password and the device identifier and is not stored on the device. If the Activation Lock has not been done previously, most MDMs have the ability to present a device Activation Lock key to the device to remove the lock via the MDM console. In the rare case that the MDM is not able to do this, AppleCare can assist in unlocking GFE devices with proof of purchase. Please work with the Apple DoD team to get this done.

2.5 Apple iOS Device Disposal

For Apple iOS devices never exposed to classified data, follow the device manufacturer's instructions (provided in Sections "Wipe on Device" and "Wipe from MDM Console" above) for wiping all user data and installed applications from the device memory, in addition to any site-specific disposal procedures.

2.6 Federal Information Processing Standard (FIPS) 140-2

Some of the cryptographic modules supporting Apple iOS 11 have not been FIPS 140-2-validated as of the date of this publication but are in process. DoD organizations using iOS 11 devices 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 iOS 10 are being revalidated to accommodate new features in Apple iOS 11. The previously validated cryptographic modules are:

- *CoreCrypto Module v7.0,* which supports applications and services such as S/MIME and HTTPS. (FIPS Certificate number 2827)
- *CoreCrypto Kernel Module v7.0,* which is used by the kernel for low-level iOS functions, such as secure boot validation and protection of data at rest (DAR). (FIPS Certificate number 2828)

2.7 Antivirus Software

Apple iOS devices do not require antivirus software. Apple iOS devices meet the virus protection requirement of DoDI 8500.01 with a combination of security policies, application sandboxing, app containers, and code signing. These technologies help contain malware and control its ability to install itself on an Apple iOS device and gain access to applications and data, device resources, and DoD networks.

2.8 Software Updates

Keeping Apple iOS up to date ensures that it has the latest enhancements and security controls in place. Apple iOS is signed and activated by Apple for each device to ensure its integrity. This STIG requires that all updates come from an approved source. Apple is considered a DoD-approved source. Apple-provided updates must be installed on Apple iOS devices when available. Apple provides the capability for DoD mobile service providers to test most updates before they are released.

2.9 Data Protection

Apple iOS encrypts all data at rest (DAR) using an inline AES 256 hardware encryption module and uses a technology called Data Protection to encrypt data stored in flash memory. When a passcode is set up on an Apple iOS device, Data Protection uses the Passcode to generate a key that is then used with the automatically enabled encryption, and when the user enters the passcode it is used to provide user authentication to then enable data decryption.

2.10 Configuration of Unmanaged Apps

Section 1.1 of the Overview document states that the scope of this STIG includes the Corporate Owned Personally Enabled (COPE) use case where both managed and unmanaged apps are supported. For the COPE use case, this version of the iOS 11 STIG implements fewer restrictions for data and apps in the personal container than previous versions of the STIG when specific conditions have been met (see next paragraph).

DoD mobile service providers may allow users full access to the Apple App Store for downloading unmanaged (personal) apps and syncing personal data on the device with personal cloud data storage accounts when ALL of the following conditions have been met:

- The site's Authorizing Official (AO) has approved full access to the Apple App Store, including downloading and installing unmanaged apps onto the iOS device and syncing personal data on the device with personal cloud data storage accounts[1]. Written approval must be available for any system compliance review.
- The site AO has provided guidance on acceptable use and restrictions, if any, on downloading and installing personal apps and data (music, photos, etc.). Guidance can be added to the user training or the User Agreement.
- Site mobile devices are configured with a work-only container technology or application that is NIAP certified. Currently iOS native managed/unmanaged app technology is the only NIAP-certified container technology or application for iOS mobile devices.
- The site MDM is configured to restrict the download of apps from all third-party app stores.
- Site mobile device users receive training on known Apple App Store application risks and STIG controls that must be enabled by the user (User Based Enforcement)[2]. See STIG requirement AIOS-11-012700 for more information.

2.11 DoD PKI Purebred

Purebred is a key management server and set of apps for mobile devices and provides a secure, scalable method of distributing software certificates for DoD PKI subscribers' use on commercial mobile devices.

[1] It is recommended that the AO provide guidance on types of apps that should be avoided in the Apple app store due to known risky functions or behaviors.
[2] UBE controls cannot be managed by the site MDM server and, therefore, must be managed by the mobile device user.

Requirements for Apple iOS devices credentialed using DoD PKI Purebred are as follows:

- Users are responsible for maintaining positive control of their credentialed devices. The DoD PKI certificate policy requires subscribers to maintain positive control of the devices that contain private keys and to report any loss of control so that the credentials can be revoked.
- Upon device retirement, turn in, or reassignment, ensure a factory data reset is performed prior to device hand-off. Follow Mobility Service Provider decommissioning procedures as applicable.

More information is available at: http://iase.disa.mil/pki-pke/Pages/purebred.aspx

3. APPLE IOS 11 TERMINOLOGY AND BEST PRACTICES

This section outlines best practices and recommendations for Apple iOS 11.

3.1 Configuration Profiles

A configuration profile is an XML file that applies configuration information to an Apple iOS device. Administrators should create a configuration profile for each Information Assurance (IA) control category (e.g., Passcode Policy, Restrictions, Managed Domain Configuration, Email, WiFi, VPN, 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 four characters plus a complex character, the user will be required to set a passcode of six characters with at least one complex character. In other words, it will enforce the combination of the more restrictive length setting from one profile and the more restrictive complexity 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 five 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. Configuration profiles that bind a device to an MDM server can be removed on non-supervised devices, but doing so will remove all managed configuration information, data, and apps, provided that the MDM configuration profile is configured to enforce this behavior.

Some configuration profiles are included with the STIG:

- Apple iOS 11 Restrictions (used to apply restrictions)
- Apple iOS 11 Passcode Policy (used to enforce password requirements)

These configuration profiles include the required and recommended values illustrated in the Configuration Tables. Where a setting is listed as optional, the default value is listed unless otherwise specified.

Organizations that use these configuration profiles should first import/transcribe them into the Apple iOS management tool of their choice and sign them to ensure integrity and nonrepudiation of source. The signed profiles can then be deployed as appropriate. This STIG provides instructions on how to manually review Apple iOS devices and configuration profiles for compliance with DoD security requirements.

3.2 Deploying Configuration Profiles

There are several ways to deploy configuration profiles depending on the use case, quantity of Apple iOS devices, and workflow:

- Using Over-the-Air configuration delivery (section titled “Over-the-Air Deployment”)
  - Using Mobile Device Management (MDM)
  - In an email message
  - From a webpage
- Using Apple Configurator (see Section title “Apple Configurator”)
- A combination of the above

3.2.1 Over-the-Air Deployment

The STIG provides verification (check) procedures and implementation guidance (fix text) that assumes an MDM tool is used to deploy configuration profiles. MDM is the preferred and expected approach for centralized management of Apple iOS devices. Alternatives to MDM are acceptable for some use cases, provided they can distribute persistent configuration profiles enforcing STIG settings.

3.2.2 Apple Configurator

An alternative to MDM is Apple Configurator, a free app on the Mac App Store. Apple Configurator requires a Mac computer running MacOS (formally called OS X) and manages Apple iOS devices through a USB or an Ethernet connection. It is a centralized management tool that can be used to set up devices (prepare and install configuration profiles), install enterprise apps, and enroll each device with an MDM solution. Apple Configurator is often used where devices need to be quickly refreshed and kept up to date with correct settings, approved policies, apps, and data. The use of Apple Configurator is most appropriate where:

- Supervision is normally enabled via the Device Enrollment Program (DEP) over the air (OTA) in conjunction with an MDM. When this is not available, Apple Configurator can supervise a device.
- The implementing organization is able to regularly update each device through physical connections or the scale of the Apple iOS deployment does not justify the expense of MDM.
- The available MDM does not support the desired configuration settings.

Apple Configurator and instructions for its use may be obtained from the Apple website.

3.3 Mobile Device Management (MDM)

MDM can be used to manage device configurations, provide administrative controls, and report on compliance. The ability of MDM to provide near real-time assessments of device configurations and remotely wipe the device makes MDM the preferred management approach wherever it is feasible. An Apple iOS device is enrolled into MDM by an administrator, end

user, or OTA via the DEP (see Section titled “Device Enrollment Program (DEP)”). Once a device is enrolled, it can receive configuration and management commands over the air.

Some MDM vendors provide an agent app for added functionality. If the agent app is removed while the device is enrolled in MDM, the management capabilities may not be affected. If the MDM enrollment profile is removed, the device can be unenrolled from MDM and all associated configuration information, managed apps, and data associated with the managed apps will also be removed. The MDM software must be configured to enforce this functionality and ensure managed apps are deleted when the enrollment profile is removed.

3.4 Apple ID

The use of Apple IDs does not pose an 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.

Note: It is recommended that DoD email addresses not be used when setting up Apple ID accounts for DoD-owned iOS devices. Instead personal email addresses should be used for the following reasons:

- DoD enterprise email systems may block important Apple ID account messages from Apple related to the service on the iOS device.
- Any Apple ID where the user knows the ID and password is considered a personal ID to Apple.

Apple IDs are not needed for remote management of a device (MDM), managed app distribution, or when applying iOS updates on the device. Apple IDs are used to personalize Apple services only.

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 the Apple iOS device for three purposes:

- Personalizing Apple Services
- Using Find My iPhone (see Section 3.6.7)
- Using iMessage or FaceTime (see Section 3.6.4)

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 iOS device 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 acceptable to use a previously created personal Apple ID on Government-furnished Apple iOS devices, provided this ID is not a member of a Family Sharing group. Family Sharing is also discussed in section titled “Family Sharing” below.

Apple IDs are protected by passcodes to prevent unauthorized use. The Apple ID passcodes are distinct from the Apple iOS device 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 iOS device to the Apple ID email address. For this reason, Apple iOS device names should not reveal a DoD affiliation, personally identifiable information (PII), or other sensitive information. Two-factor authentication is also available with Apple IDs and it is recommended, but not required, that users consider using two-factor authentication.

3.5 Apps

3.5.1 Apple App Store

The App Store is an application distribution platform for Apple iOS apps. Apps in the App Store are reviewed by Apple and digitally signed for use on Apple iOS devices. Not all of the applications in the App Store are appropriate for use on Government-Furnished Equipment (GFE). DoD organizations must establish their own approval processes to determine which applications are appropriate for their use cases.

Applications purchased with an Apple ID are available to other Apple iOS devices configured with the same Apple ID. Previously purchased applications will not automatically download on a new device when an existing Apple ID is associated with it. Users should be discouraged from subsequently synchronizing applications across personally owned and Government-furnished Apple iOS devices. To prevent applications acquired for personal use from automatically downloading on a Government-furnished Apple iOS device, the user should turn off "Apps" under "AUTOMATIC DOWNLOADS" in the "iTunes & App Store" section of the Settings app on the Apple iOS device.

3.5.2 Managed Apps

Managed apps are applications installed through an MDM. Once installed, the MDM server can enforce additional restrictions on these apps. Apps that store DoD data should be managed via an MDM where possible. Managed apps give DoD organizations the ability to keep DoD documents contained within Managed apps and prevent non-DoD documents from being opened in managed apps. Managed apps are subject to MDM control for:

- Use of iCloud document storage
- Ability to back up application data via USB and iCloud
- Per-app VPN
- Single sign-on
- App configuration
- Removal on MDM unenrollment

3.5.3 Enterprise Apps

Enterprise (or in-house) apps are Apple iOS apps developed for internal deployment within an organization. Enterprise apps are not reviewed by Apple and are deployed outside of the Apple App Store. Enterprise apps must be vetted and approved before they are installed on Apple iOS devices. Enterprise apps can be deployed using MDM, Apple Configurator, email, or a web server. Deploying enterprise apps via MDM will designate them as managed apps and permit them to have access to DoD documents.

3.5.4 App Extensions

An App Extension (Extension) is used to extend a specific function of an app and make it available to users while they are using other apps. There are several types of Extensions:

- Share: Post to a sharing website or share content with others
- Document Provider: Provide remote storage of iOS user documents that then can be used by compatible apps
- Photo Editing: Edit a photo or video within the Photos app
- Today: Get a quick update or perform a quick task in Today view or Notification Center
- Action: Manipulate or view content within the context of another app
- Custom Keyboard: Use a custom keyboard instead of Apple iOS system keyboard
- File Provider: A local file repository that can be accessed by other apps
- Audio: Provide audio effects, sound generators, and musical instruments

Extensions are bundled and distributed with apps. For example, if a user downloads a photo editing app that includes the Photo Editing Extension Point, the user will be able to access defined editing features from the photo editing app within the native Apple iOS Camera app.

When vetting apps for DoD, Extensions need to be tested and accounted for. While there is no ability to turn off Extensions through an Apple iOS management tool, they respect “Managed open in” controls. For example, a custom keyboard installed directly from the App Store can be prevented from use in a managed app.

3.6 Apple iOS Capabilities and Restrictions

This section reviews selected capabilities in Apple iOS 11 that have IA implications or restrictions.

3.6.1 WiFi

WiFi is available for use on Apple iOS devices. The WiFi client is WiFi Protected Access 2 (WPA2) certified. Apple iOS supports multiple types of Extensible Authentication Protocol (EAP), including EAP-TLS. Users can turn WiFi on or off from the Control Center. WiFi cannot be deactivated using MDM. DoD organizations that want to specify restrictions for connections to particular WiFi access points can do so through a configuration profile.

3.6.2 Bluetooth

The Apple iOS Bluetooth stack supports seven Bluetooth profiles. The Phone Book Access Profile (PBAP) functions are only available on iPhones. Users can turn Bluetooth on or off from the Control Center. Apple publishes a list of the profiles and their use at: https://support.apple.com/en-us/HT204387

The Personal Area Networking (PAN) Profile allows the Apple iOS device to establish a Bluetooth network with one or more Bluetooth-capable devices, such as PCs, tablets, or smartphones. Because it is only enabled by apps, and not the OS, access to the profile is controlled through the app approval process.

3.6.3 Email

The native Apple iOS 11 email app (Mail) is authorized for the receipt and transmission of DoD email messages when used with a DoD Enterprise Email account and can also enable Secure/Multipurpose Internet Mail Extensions (S/MIME) via derived credentials. The DoD account should be configured using MDM, which makes it a managed account, ensuring email attachments cannot be opened in unmanaged apps.

The Mail app is permitted for personal email accounts at the discretion of the local command. To prevent email attachments in personal email messages from being opened in managed apps, personal email accounts must be configured by the user of the Apple iOS device and not by MDM. Local commands permitting personal email accounts are advised to include statements in the user agreement concerning a user's expectation of privacy in personal email stored, received, or transmitted from Apple iOS devices.

DoD organizations that require a CAC for signing messages and reading encrypted email must use either an authorized derived credential in Apple iOS native Mail or a third-party email app.

3.6.3.1 Web Browser

The Apple iOS native web browser (Safari) supports the use of certificate-based authentication but does not support third-party CAC readers for certificate-based authentication. Safari is a

hybrid app. All non-managed domains are not able to share documents with managed apps, per the setting defined in the configuration table, while managed domains are able to share documents (see section titled “Managed Domains”). Use of authorized derived credentials with Safari or a third-party CAC-enabled browser may be required to access DoD CAC-authenticated websites (see section titled “Managed Apps”).

3.6.3.2 Managed Domains

In Apple iOS 11, the native Safari browser allows for the use of managed domains. Managed domains are trusted web domains specified in a configuration profile by the Apple iOS management tool. Apple iOS devices can move documents and media between managed domains and managed apps. A list of DoD domains can be obtained from the DoD Network Information Center (NIC) (see https://www.nic.mil).

3.6.3.3 AirPlay

AirPlay allows a user to wirelessly stream content from his or her Apple iOS device 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 iOS devices to the Apple TV.

3.6.4 iMessage, FaceTime, and Apple Push Notification Service

iMessage, FaceTime, and Apple Push Notification Service (APNS) are encrypted and authenticated communication tools approved for DoD use. iMessage and FaceTime are native apps on Apple iOS. iMessage is not authorized for the transmission of For Official Use Only (FOUO) information.

3.6.5 Siri

Siri enables a user to use his or her voice to query or instruct the Apple iOS device for a variety of purposes, including sending messages, scheduling meetings, obtaining information, setting alarms, and placing phone calls. Use of Siri is allowed but must be disabled at the lock screen to protect PII and sensitive data that might have been improperly stored in the contacts or calendar apps.

3.6.6 Virtual Private Network (VPN)

Apple iOS devices support multiple types of VPN technologies, including IPsec, IKEv2, and SSL. Authentication to a VPN can be achieved using a username and password or certificates where authorized. To connect to a VPN requiring CAC authentication, connect using derived credentials or install a third-party CAC-enabled VPN client. Apple iOS also supports session-based (per app VPN) connections with managed apps.

3.6.7 iCloud

iCloud is a suite of services that enables a user to access content from multiple Apple iOS devices. It is approved in DoD for the limited purposes of:

- Synchronization of personal email, contacts, and calendars
- Facilitating location of a lost or stolen device ("Find My iPhone")
- Backup of unmanaged apps and data (see section titled "Managed Apps" on how to disable iCloud on managed Apps)

If "Find My iPhone" is enabled, the user must disable it before the organization can repurpose the Apple iOS device (see section titled "Deprovisioning").

The following iCloud services are not permitted in DoD unless approved by the AO when unrestricted use of unmanaged apps is allowed:

- iCloud Backup of unmanaged data (use with managed apps is always disapproved)
- My Photo Stream
- Photo Sharing
- iCloud Photo Library
- iCloud Keychain
- iCloud Documents and Data of unmanaged data (use with managed apps is always disapproved)
- iCloud Drive

3.6.8 Touch ID

Touch ID is the fingerprint sensing system that can be used to unlock an Apple iOS device and authorize purchases in iTunes, iBooks, and App Stores. Touch ID authorization is based on Local AO approval.

Version 3.1 of the Protection Profile for Mobile Device Fundamentals includes design requirements and assurance activities for biometric authentication systems.

To date, no evaluation has been conducted on the biometric components of the Touch ID system; therefore, any AO implementing Touch ID may be accepting an unknown risk.

3.6.9 Face ID

Face ID is a facial recognition system that can be used to unlock an Apple iOS device and authorize purchases in iTunes, iBooks, and App Stores. Face ID authorization is based on Local AO approval.

Version 3.1 of the Protection Profile for Mobile Device Fundamentals includes design requirements and assurance activities for biometric authentication systems.

To date, no DoD organization has been able to test Face ID and it has not been evaluated via the Common Criteria process. It is recommended that AOs not deploy Face ID until independent evaluation data is available concerning the performance of this feature.

Note: The single control "Allow Touch ID to unlock device" enables/disables both Touch ID and Face ID. Because separation of controls is not possible, it is recommended that Face ID-capable iOS devices (iPhone X) be placed in a separate management group from all other iOS devices. This separate management group would have "Allow Touch ID to unlock device" disabled in order to disable Face ID. The other iOS devices, being those which do not support Face ID, can have this feature enabled as it would only permit Touch ID.

3.6.10 Share My Location

Share My Location shares a device's location using the iMessages and Find My Friends apps. If multiple devices use a single Apple ID, only one selected location is shared. DoD devices must not be used with Share My Location.

3.6.11 Family Sharing

Family Sharing allows up to six invited Apple IDs to join a "Family Group". Members of this Family Group can:

- Share a single payment method for iTunes, App Store, and iBooks
- Share a common Family calendar and reminder list
- Share a Family photo stream
- Use Find iPhone to perform remote functions such as lock, wipe, or play a sound on a Family Member's device
- Use Shared Locations in Messages, Find My Friends, and Find My iPhone to locate a device for an individual Family Member

Apple IDs used in DoD must not be configured with Family Sharing. Disabling Family Sharing on an Apple ID will disable it on all devices using that Apple ID.

3.6.12 HealthKit

The new Health app gives users an easy-to-read dashboard of their health and fitness data. Health includes a Medical ID that can be viewed while the Apple iOS device is locked in case of emergency. The Medical ID can include PII information such as name, birthday, blood type, medications, height, weight, and emergency contacts. The Medical ID can display information to any user that picks up the Apple iOS device, similar to a medical alert ID bracelet or necklace. Medical ID should be used with the same restrictions as a medical alert ID.

3.6.13 AirPrint

AirPrint provides the capability for wired and wireless printing from an Apple iOS device. Setting up wireless printing from a mobile device to a DoD network-connected printer is problematic due to the print server requirements listed in the MultiFunction Device STIG and the DoD WiFi network requirements listed in the Network Infrastructure STIG. DoD iOS device users connected to DoD network can use AirPrint to network print servers/printers.

3.6.14 Apple Watch

The use of Apple Watch with iOS 11 devices is prohibited at this time. DISA has not yet completed a risk assessment of Apple Watch Series 3 watches, watchOS 4, or the new capability of some Watch apps to operate disconnected from the iPhone version of the same app. The STIG will be updated based on the results of this risk assessment.

3.6.15 Device Enrollment Program (DEP)

The Device Enrollment Program (DEP) provides a streamlined way to deploy Government-owned Apple iOS devices. DEP allows end users or central IT to take a Government-owned Apple iOS device out of the box, enroll it into MDM, and supervise it over the air. Additionally, if a device is enrolled in an MDM through DEP, removal of MDM can be prevented. In order to use DEP, devices need to be purchased directly from Apple, participating Apple Authorized Resellers (including carriers), or manually added via a Mac and Apple Configurator 2.5.

4. OPERATIONS CONSIDERATIONS

4.1 Hand Receipt and Acceptable Use Policy

When distributing Apple iOS devices to end users, a hand receipt is required. The hand receipt should detail the DoD acceptable terms of use. Some MDM vendors make it possible to display a "Terms of Use" policy when enrolling into MDM; however, this is only done one time and should not be the sole means for a user to accept the "Terms of Use".

4.2 End User Training

This STIG requires some User-Based Enforcement (UBE) controls, meaning there is no server-based configuration setting available to enable/disable a specific IA control. On the Apple iOS device, the following UBE controls must be enforced:

- Remove Family Sharing
- Disable Shared Location
- Turn off "Apps" under "AUTOMATIC DOWNLOADS" in the "iTunes & App Store" section of the Settings app on the Apple iOS device

The Apple iOS device's single persona is for business purposes only. The following are best practices for end users acting as stewards of DoD data:

- No sensitive data should be in the Contacts or Calendar apps
- Do not synchronize contacts and calendar information to Bluetooth peripherals
- Do not use iMessage for FOUO information
- The device name should not expose affiliation to the DoD
- Do not copy/paste data outside managed apps
- Do not store sensitive DoD audio tracks in the Music app

4.3 Deprovisioning

A deprovisioning process is required for Apple iOS devices at end of life or when an employee transitions to another role. Deprovisioning is the act of unenrolling a device from management, deleting the current user's accounts, and wiping all data from the device.

Apple iOS includes a feature called Activation Lock, which makes it difficult for anyone to use or sell an Apple iOS device that has been lost or stolen. Activation Lock is enabled by signing into iCloud on a device and turning on "Find My iPhone". As part of the deprovisioning process, it is necessary for the end user to remove his or her iCloud account or turn off "Find My iPhone" from the device, thereby disabling Activation Lock. This can also be accomplished by selecting "Erase All Content and Settings" from within the Settings application on the device and completing a device wipe. See sections titled "Wipe on Device", "Activation Lock", and "Wipe from MDM Console".