

UNCLASSIFIED



# **APPLE IOS/IPADOS 18 SUPPLEMENTAL PROCEDURES**

**Version 2, Release 4**

**30 September 2026**

**Developed by Apple and DISA for the DoW**

UNCLASSIFIED

### **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 the Defense Information Systems Agency (DISA) of any nonfederal entity, event, product, service, or enterprise.

## TABLE OF CONTENTS

|                                                                           | Page      |
|---------------------------------------------------------------------------|-----------|
| <b>1. MOBILE DEVICE PROCEDURES .....</b>                                  | <b>1</b>  |
| 1.1 Apple iOS Wipe Procedures .....                                       | 1         |
| 1.2 Wipe on Device.....                                                   | 1         |
| 1.3 Activation Lock.....                                                  | 1         |
| 1.4 Wipe from MDM Console .....                                           | 1         |
| 1.5 Apple iOS Device Disposal.....                                        | 2         |
| 1.6 Federal Information Processing Standard (FIPS) 140-2/140-3.....       | 2         |
| 1.7 Antivirus Software .....                                              | 2         |
| 1.8 Software Updates .....                                                | 2         |
| 1.9 Configuration of Unmanaged Apps.....                                  | 2         |
| 1.10 DoW PKI Purebred .....                                               | 3         |
| <b>2. APPLE INTELLIGENCE INFORMATION .....</b>                            | <b>4</b>  |
| <b>3. APPLE IOS/IPADOS 18 TERMINOLOGY AND BEST PRACTICES.....</b>         | <b>6</b>  |
| 3.1 Configuration Profiles .....                                          | 6         |
| 3.2 Apple ID .....                                                        | 6         |
| 3.3 Apps.....                                                             | 7         |
| 3.3.1 Apple App Store.....                                                | 7         |
| 3.3.2 Managed Apps .....                                                  | 8         |
| 3.3.3 Enterprise Apps.....                                                | 8         |
| 3.4 Apple iOS Capabilities and Restrictions.....                          | 9         |
| 3.4.1 Wi-Fi .....                                                         | 9         |
| 3.4.2 Bluetooth.....                                                      | 9         |
| 3.4.3 Email .....                                                         | 9         |
| 3.4.4 Web Browser .....                                                   | 9         |
| 3.4.5 Managed Domains .....                                               | 10        |
| 3.4.6 AirPlay.....                                                        | 10        |
| 3.4.7 iMessage, FaceTime, and Apple Push Notification Service (APNS)..... | 10        |
| 3.4.8 Siri.....                                                           | 10        |
| 3.4.9 Virtual Private Network (VPN) .....                                 | 10        |
| 3.4.10 iCloud.....                                                        | 10        |
| 3.4.11 Touch ID.....                                                      | 11        |
| 3.4.12 Face ID .....                                                      | 11        |
| 3.4.13 Share My Location .....                                            | 11        |
| 3.4.14 Family Sharing .....                                               | 11        |
| 3.4.15 AirPrint .....                                                     | 12        |
| 3.4.16 Apple Watch .....                                                  | 12        |
| 3.4.17 Apple Business Manager (ABM).....                                  | 12        |
| 3.4.18 Continuity.....                                                    | 12        |
| <b>4. OPTIONAL CONSIDERATIONS .....</b>                                   | <b>13</b> |
| 4.1 Hand Receipt and Acceptable Use Policy.....                           | 13        |
| 4.2 End-User Training.....                                                | 13        |

|     |                     |    |
|-----|---------------------|----|
| 4.3 | Deprovisioning..... | 13 |
|-----|---------------------|----|

## 1. MOBILE DEVICE PROCEDURES

### 1.1 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/iPadOS devices never exposed to classified data.

### 1.2 Wipe on Device

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

To wipe the device, perform the following steps:

1. Open the **Settings** app.
2. Tap **General**.
3. Tap **Transfer or Reset iPhone**.
4. Tap **Reset**.
5. Tap **Reset All Settings**.
6. Enter the device unlock passcode and, if used, the iCloud passcode.

### 1.3 Activation Lock

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

1. Go to **www.iCloud.com/find**.
2. Sign in with your Apple ID and password.
3. Select the device you want to remove from iCloud.
4. Click **Remove This Device**.

Activation Lock is also removed if the device is wiped via the on-device wipe method described above. It is not removed if the device is wiped via the Mobile Device Management (MDM) wipe device command.

### 1.4 Wipe from MDM Console

If the wipe is being performed as part of a reprovisioning process, the user or administrator must 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 **Wipe** 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. This can only be done if the device was supervised by the MDM and the MDM requested the unlock key from the device. In the rare case the MDM is not able to do this, AppleCare can assist in unlocking government-furnished equipment (GFE) devices with proof of purchase. Work with the Apple DoW team if this occurs.

## 1.5 Apple iOS Device Disposal

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

## 1.6 Federal Information Processing Standard (FIPS) 140-2/140-3

FIPS 140-3 validation for iOS/iPadOS 18 cryptographic modules is in process.

For DoW organizations using iOS/iPadOS 18 devices, visit the following website for updates on the validation status: <https://csrc.nist.gov/Projects/cryptographic-module-validation-program/Validated-Modules/Search>.

Modules that are in process can be found at <https://csrc.nist.gov/Projects/cryptographic-module-validation-program/modules-in-process/Modules-In-Process-List>.

## 1.7 Antivirus Software

Apple iOS devices do not require antivirus software. Apple iOS/iPadOS 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 the ability to self-install on an Apple iPhone and iPad to gain access to applications and data, device resources, and DoW networks.

## 1.8 Software Updates

Keeping Apple iOS/iPadOS up to date ensures the latest enhancements and security controls are in place. Apple iOS/iPadOS is signed and activated by Apple for each device to ensure integrity. This STIG requires that all updates come from an approved source. Apple is considered a DoW-approved source. Apple-provided updates must be installed on Apple iPhones and iPads when available. Apple provides the capability for DoW mobile service providers to test most updates before release via the AppleSeed program.

## 1.9 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/iPadOS 18 STIG implements fewer restrictions for data and apps in the personal container than previous versions of the STIG when specific conditions have been met as outlined below.

DoW mobile service providers may allow the user 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<sup>1</sup>. 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)<sup>2</sup>. Refer to STIG requirement AIOS-18-011900 for more information.

### 1.10 DoW PKI Purebred

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

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

- The Purebred Registration app must be installed as a managed app on iOS devices via enterprise management, and the "Allow documents from managed sources in unmanaged destinations" restriction must be enforced by the policy to limit apps that can leverage key sharing.
- Users are responsible for maintaining positive control of their credentialed devices. The DoW PKI certificate policy requires subscribers to maintain positive control of the devices that contain private keys and report any loss of control so the credentials can be revoked.
- Upon device retirement, turn in, or reassignment, ensure a factory data reset is performed prior to device handoff. Follow procedures in the [Deprovisioning](#) section and any other procedures defined by the DoW Management Service Provider.

More information is available at <https://cyber.mil/pki-pke/>.

---

<sup>1</sup> 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.

<sup>2</sup> UBE controls cannot be managed by the site MDM server and therefore must be managed by the mobile device user.

## 2. APPLE INTELLIGENCE INFORMATION

Apple Intelligence is Apple’s implementation of artificial intelligence (AI) within the Apple ecosystem. Apple Intelligence uses generative AI to help users work, communicate, and express themselves. Apple Intelligence is built into iOS 18, iPadOS 18, and macOS Sequoia and found in many Apple apps, including Writing tools, notifications, Mail, and Siri.

Apple Intelligence tasks are processed either on device or on Apple servers in the cloud in a private, Apple-managed area called Private Cloud Compute (PCC). Whether the Apple Intelligence request is processed on device or by PCC depends on the processing needs of the Apple Intelligence request. Apple Intelligence will support supplemental third-party AI services, with ChatGPT being the first one supported (late 2024). **The STIG requires Apple Intelligence supplemental third-party AI services be disabled (refer to requirement AIOS-18-015400).** In addition, most Apple Intelligence features with specific management APIs (for example, “Image Wand”) have also been disabled in the STIG.

As previously stated, Apple Intelligence is fully integrated into iOS, iPadOS and macOS, and many Apple apps. The Enterprise cannot disable processing DoW data in the cloud via PCC via a mobile device manager (MDM) server, but the user can disable this on the device.

Apple has released a PCC security guide that describes details of the security infrastructure Apple used when setting up PCC. The Private Cloud Compute Security Guide can be found here: <https://security.apple.com/documentation/private-cloud-compute>. Some highlights of PCC security include:

- Stateless computation on personal user data
  - A user’s device sends data to PCC for the sole, exclusive purpose of fulfilling the user’s inference request. PCC uses that data only to perform the operations requested by the user.
  - User data is encrypted directly to the PCC nodes that are processing the request, and the decrypted user data is retained only until the response is returned.
  - User data is never available to Apple—even to staff with administrative access to the production service or hardware.
  - End-to-end encryption is used between the mobile device and PCC.
  - The root of trust for PCC is Apple’s compute node: custom-built server hardware that brings the power and security of Apple silicon to the data center, with the same hardware security technologies used in iPhone, including the Secure Enclave and Secure Boot.
- Enforceable guarantees: PCC does not depend on external components for its core security and privacy guarantees.
  - The Secure Enclave randomizes the data volume’s encryption keys on every reboot and does not persist these random keys, ensuring data written to the data volume cannot be retained across reboot.
- No privileged runtime access: PCC does not contain privileged interfaces that would enable Apple’s site reliability staff to bypass PCC privacy guarantees, even when working to resolve an outage or other severe incident.

- Non-targetability: An attacker cannot attempt to compromise personal data that belongs to specific, targeted PCC users without attempting a broad compromise of the entire PCC system.
  - Technologies such as Pointer Authentication Codes and sandboxing act to resist such exploitation and limit an attacker's horizontal movement within the PCC node.
- Verifiable transparency: Apple will provide access to PCC to security researchers so they can verify, with a high degree of confidence, that Apple's privacy and security guarantees for Private Cloud Compute match their public promises.

### 3. APPLE IOS/IPADOS 18 TERMINOLOGY AND BEST PRACTICES

This section outlines best practices and recommendations for Apple iOS/iPadOS 18.

#### 3.1 Configuration Profiles

A configuration profile is an XML file that applies configuration information to an Apple iOS device. Administrators must create a configuration profile for each Information Assurance (IA) control category (e.g., Passcode Policy, Restrictions, Managed Domain Configuration, email, Wi-Fi, VPN, etc.), rather than a single profile containing all potential settings. The use of multiple profiles allows for flexible updates without affecting standard configurations.

Organizations must first import/transcribe configuration profiles into an Apple iOS management tool and then sign the profile 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 DoW security requirements.

#### 3.2 Apple ID

Two types of Apple IDs are available for use in the DoW: Personal Apple IDs and Managed Apple IDs. The DoW currently uses Personal Apple IDs on all iOS devices with Apple IDs. Prior to the availability of managed Apple IDs (announced at the 2019 Apple Worldwide Developers Conference), only personal Apple IDs were available. Apple IDs with DoW-affiliated domain names are considered Personal Apple IDs if the user has the current passcode and the device is not managed via Apple Business Manager (required for Managed Apple IDs).

The use of Personal Apple IDs does not pose an IA risk when applications containing DoW-sensitive information are managed appropriately. Personal Apple IDs are not designed to be managed by an organization, and no tools are provided to accomplish such administration. DoW organizations must avoid issuing organizationally generated Apple IDs using DoW email domain names.

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

An Apple ID serves as the username for the iTunes Store, App Store, iCloud, and other Apple services. In the DoW, an Apple ID is needed on the Apple iOS device for three purposes:

- Personalizing Apple Services.
- Using Find My iPhone.
- Using iMessage or FaceTime.

To obtain a Personal Apple ID, the user must agree to Apple's Terms and Conditions. DoW cannot serve as a proxy for a user's acceptance of the Terms and Conditions. Users can create a Personal Apple ID on the Apple iOS device or online at <https://appleid.apple.com>. An Apple knowledge base article at <https://support.apple.com/en-us/HT204316> explains how to create an Apple ID. 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 discussed 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 are encouraged to select Apple ID passcodes within DoW guidelines. For example, the following rules should be used:

- Be at least 15 characters long.
- Contain at least one uppercase alphabetic character.
- Have at least one lowercase 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 Personal Apple ID email address. For this reason, Apple iOS device names must not reveal a DoW affiliation, personally identifiable information (PII), or other sensitive information. Two-factor authentication, available with Personal Apple IDs, is recommended but not required.

Managed Apple IDs are created by the organization with Apple Business Manager or a federated sync with an existing directory service provider, such as Entra ID and Office 365. All IDs created via Apple Business Manager are referred to as Managed Apple IDs. Organization administrators can perform functions typical of other organizational IDs on Managed Apple IDs.

Two primary types of Managed Apple IDs are used in the DoW. Currently, the DoW uses administrative Apple IDs to manage programs and access Apple IT systems sites such as <https://business.apple.com>.

The second type of Managed Apple ID is similar to a Personal Apple ID employed by an end user for personalization of an iOS device. The organization retains ownership of Managed Apple IDs, and some functions of personalization can be limited. Additionally, functions such as commerce interactions with Apple may be limited, and interactions with other Apple IDs may be restricted.

Managed IDs may use a different email domain than the organization's typical email domain. Apple recommends that organizations differentiate the Managed Apple ID from the standard organization email address. For example, if the organization's email domain is user@service.mil, the Managed Apple ID might be user@appleid.service.mil. This Managed Apple ID does not have to correspond to an actual email address in the organization.

Additionally, when the Managed Apple ID is created, the user's standard email address is associated with the ID but is not required to be the Apple ID. Managed Apple IDs give the organization ID management functions, including resetting passwords and managing connections to the federated ID system.

### 3.3 Apps

#### 3.3.1 Apple App Store

The App Store is an application distribution platform for Apple iOS and iPadOS apps. Apps in the App Store are reviewed by Apple and digitally signed for use on Apple iPhones and iPads. Because not all of the applications in the App Store are appropriate for use on GFE, DoW organizations

must establish approval processes to determine which applications are permitted. DoW Chief Information Officer Memorandum “Mobile Application Security Requirements,” October 6, 2017, provides guidance on app vetting/review requirements for both management (work) and unmanaged (personal) apps.

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 are discouraged from synchronizing applications across personally owned and government-furnished Apple iPhones and iPads. To prevent applications acquired for personal use from automatically downloading on government-furnished Apple iPhones and iPads, the user must turn off **Apps** under **Automatic Downloads** in the **iTunes & App Store** section of the **Settings** app on the Apple device.

### 3.3.2 Managed Apps

Managed apps are installed through an MDM. After installation, the MDM server can enforce additional restrictions on these apps. Apps that store DoW data must be managed via an MDM where possible. Managed apps give DoW organizations the ability to keep DoW documents contained within managed apps and prevent non-DoW 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.

### 3.3.3 Enterprise Apps

Enterprise (or in-house) apps are Apple iOS/iPadOS 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 installation on Apple 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 DoW documents.

Custom Apps (previously known as B2B apps) are developed by organizations for internal use but distributed via the Apple App Store. Custom apps are reviewed by Apple (similar to consumer apps) but are not available without being explicitly assigned to the organization’s Apps and Books

account. These apps are not searchable on the app store. Custom apps can be made available to mission partners and other services within the guidelines of the Apple Custom App distribution agreement. Apps developed by one service can be shared with another service without having to transfer the App’s source code. These apps can be distributed via an MDM and can also be managed.

### 3.4 Apple iOS Capabilities and Restrictions

This section reviews selected capabilities in Apple iOS/iPadOS 18 that have IA implications or restrictions.

#### 3.4.1 Wi-Fi

Wi-Fi is available for use on Apple devices. The Wi-Fi client is Wi-Fi Protected Access 3 (WPA3) certified. Apple iOS/iPadOS supports multiple types of Extensible Authentication Protocol (EAP), including EAP-TLS. Users can turn Wi-Fi on or off from the Control Center. Wi-Fi cannot be deactivated using MDM; however, it can be configured and controlled on supervised devices. DoW organizations that want to specify restrictions for connections to particular Wi-Fi access points can do so through a configuration profile. Apple devices achieved Common Criteria Validation against the Wireless LAN Client Protection Profile version 1.0 cc version 3.1 on 10 October 2023 (CCEVS-VR-VID11349-2023).

#### 3.4.2 Bluetooth

The Apple iOS/iPadOS Bluetooth stack supports nine 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>. Two profiles are the Wireless iPhone Accessory Protocol (WiAP) and Braille. The other seven supported profiles are HFP 1.6, PBAP, A2DP, AVRCP 1.4, PAN, HID, and MAP.

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.

#### 3.4.3 Email

The native Apple iOS/iPadOS 18 email app (Mail) is authorized for the receipt and transmission of DoW email messages when used with a DoW Enterprise Email account and can also enable Secure/Multipurpose Internet Mail Extensions (S/MIME) via derived credentials. The DoW account must be configured using MDM, classifying it as a managed account to ensure 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 iPhone and iPad 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 devices.

DoW organizations that require a CAC for signing messages and reading encrypted email must use an authorized derived credential (e.g., Purebred).

#### 3.4.4 Web Browser

The Apple iOS/iPadOS native web browser (Safari) supports the use of certificate-based authentication (e.g., using Purebred installed certificates). Safari is a hybrid app. All non-managed

domains are not able to share documents with managed apps, while managed domains are able to share documents (refer to the [Managed Domains](#) section of this document). Use of authorized derived credentials with Safari or a third-party CAC-enabled browser may be required to access DoW CAC-authenticated websites (refer to [Managed Apps](#) section of this document).

Refer to <https://www.niap-ccevs.org/Profile/Info.cfm?PPID=378&id=378>.

### 3.4.5 Managed Domains

In Apple iOS/iPadOS 18, 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/iPadOS management tool. Apple devices can move documents and media between managed domains and managed apps. A list of DoW domains can be obtained from the DoW Network Information Center (NIC) at <https://www.nic.mil>.

### 3.4.6 AirPlay

AirPlay allows a user to stream content wirelessly from an Apple 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 must be configured to use an onscreen code. Users must enter the code each time data is transmitted from an Apple iOS device to the Apple TV.

### 3.4.7 iMessage, FaceTime, and Apple Push Notification Service (APNS)

FaceTime, iMessage, and APNS are encrypted and authenticated communication tools approved for DoW use. FaceTime and iMessage are native apps on Apple iOS/iPadOS. iMessage is not authorized for the transmission of Controlled Unclassified Information (CUI) due to the inability of the sender to positively identify on which end devices the messages are received. FaceTime has been disabled in the STIG.

### 3.4.8 Siri

Siri allows a user, via voice command, 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.

### 3.4.9 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/iPadOS also supports session-based (per-app VPN) connections with managed apps.

### 3.4.10 iCloud

iCloud is a suite of services that enables a user to access content from multiple Apple iOS devices. It is approved in DoW 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 (refer to the Managed Apps section 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 (refer to the Deprovisioning section).

The following iCloud services are permitted in DoW if 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.

#### **3.4.11 Touch ID**

Touch ID is the fingerprint sensing system used to unlock an Apple iOS device and authorize purchases in iTunes, iBooks, and App Stores.

Touch ID was approved for use after being evaluated via the Common Criteria process during the successful iOS 12 evaluation.

#### **3.4.12 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 was approved for use after being evaluated via the Common Criteria process during the successful iOS 12 evaluation.

#### **3.4.13 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. DoW devices must not be used with Share My Location.

#### **3.4.14 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 My 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 DoW must not be configured with Family Sharing. Disabling Family Sharing on an Apple ID will disable it on all devices using that Apple ID.

### 3.4.15 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 DoW network-connected printer is problematic due to the print server requirements listed in the Multifunction Device STIG and the DoW Wi-Fi network requirements, as detailed in the Network Infrastructure STIG. AirPrint use is disabled in the STIG.

### 3.4.16 Apple Watch

The use of Apple Watch is disabled in the STIG.

### 3.4.17 Apple Business Manager (ABM)

Apple Business Manager (ABM) is the name for the single management interface to the former Device Enrollment Program (DEP) and the Volume Purchase Program (VPP). The ABM interface provides a seamless way for DoW organizations to access both devices and app data with a single

managed set of Managed Apple IDs. Within ABM, the former DEP (now called "Automatic Device Enrollment") and VPP (now called "Apps and Books") are available and allow for further location-specific management as well as future program enhancements.

Automatic Device Enrollment provides a streamlined way to deploy government-owned Apple iOS devices. This allows end users or central IT to take a government-owned Apple iOS device out of the box, enroll it in an MDM, and supervise it over the air. Additionally, if a device is enrolled in an MDM through ABM, removal of MDM can be prevented. To use Automatic Device Enrollment, devices must be purchased directly from Apple or participating Apple Authorized Government Resellers (including cellular carriers) or manually added via a Mac and the free Apple Configurator 2 application.

### 3.4.18 Continuity

When a user is signed into the same Apple ID on different Apple devices (iOS, iPadOS, macOS), Continuity allows the user to move seamlessly among those devices. Tools such as Handoff, Universal Clipboard, Instant Hotspot, Auto Unlock, Sidecar, and iPhone Mirroring on Mac are enabled via Continuity. Continuity uses technologies such as iCloud, Bluetooth, and Wi-Fi to enable the passing of activity from one device to another, make and receive phone calls, send and receive text messages, and share a cellular internet connection. Use of Continuity features that require iCloud will require AO approval for iCloud.

Continuity is disabled in the STIG.

## 4. OPTIONAL CONSIDERATIONS

### 4.1 Hand Receipt and Acceptable Use Policy

When distributing Apple devices to end users, a hand receipt is required. The hand receipt should detail the DoW 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 once 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 no server-based configuration setting is available to enable/disable a specific IA control. On the Apple 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 device’s single persona is for business purposes only. The following are best practices for end users acting as stewards of DoW data:

- Do not include sensitive data in the Contacts or Calendar apps.
- Do not synchronize contacts and calendar information to Bluetooth peripherals.
- Do not use iMessage for CUI information.
- Do not name the device in a way that exposes affiliation with the DoW.
- Do not copy/paste data outside managed apps.
- Do not store sensitive DoW audio tracks in the Music app.

### 4.3 Deprovisioning

A deprovisioning process is required for Apple iOS/iPadOS 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.

The Apple feature, Activation Lock, makes it difficult for anyone to use or sell an Apple iOS/iPadOS device that has been lost or stolen. Activation Lock is enabled by signing in to iCloud on a device and turning on Find My iPhone. As part of the deprovisioning process, the end user must remove the 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. Refer to sections [Wipe on Device](#), [Activation Lock](#), and [Wipe from MDM Console](#).