What This Guide Provides

This pamphlet provides security recommendations for users of personally managed Apple iPhones and iPads running iOS 5. This refers to a situation in which the user exercises sole administrative control over the device.

This pamphlet does not address the security and configuration issues involved with integrating iOS devices into enterprise environments, in which the enterprise would select a mobile device management product, require certain settings, and monitor device status. Enterprise deployment issues such as the management of configuration profiles, network infrastructure settings, connecting to VPNs, and Exchange ActiveSync, are discussed on Apple's website at http://www.apple.com/support/iphone/enterprise/.

Maintain Physical Security

Always maintain physical control of your iOS device. All electronic devices are subject to physical attacks, but the portable nature of smartphones and tablets puts them at particular risk. Publicly available tools can allow an attacker with physical access to your device to bypass some of its security mechanisms.

The best protection against physical attacks is to ensure that your iOS device never falls into the wrong hands. Consider the risks of storing sensitive data on your device. This includes corporate information, credit card numbers, saved passwords, and personal data. Although the Data Protection feature is used by some apps to provide cryptographic protection to data at rest, other apps which store sensitive data do not use it.

Apply the Latest Software Updates

Always apply the latest software updates for iOS, as these include important security patches. Previous versions of iOS required that the device be connected to a computer running iTunes, but with iOS 5 it is now possible to apply the updates directly to the device from Apple.

Go to Settings > General > Software Update

The device will automatically search for available software updates. If an update is available, apply it. It is the responsibility of the individual user to ensure that the device has the latest version of iOS. Regularly check for software updates for iOS.

If the device is running an older version of iOS and the Software Update option is not available, it will first be necessary to update the device to iOS 5 by connecting it to a trusted computer running the latest version of iTunes. Once iOS 5 is installed, use the Software Update pane on the device to apply all future updates.

Do Not Jailbreak Your iPhone or iPad

"Jailbreaking" is the term that refers to the process of modifying the iOS device's operating system in violation of the end-user license agreement. Jailbreaking significantly damages the device's ability to resist attacks because it disables the enforcement of code signatures, which is an important security feature. Jailbreaking an iPhone or iPad makes an attacker's job substantially easier. Many publicly-released attacks targeted at iOS devices require that they first be jailbroken.

Another concern related to jailbreaking is the quality of the tools and applications provided by the jailbreaking community. These free applications are developed with little oversight and limited testing. They may include viruses or other malware, and they may inflict lasting harm on your device by breaking it permanently or corrupting your data.

Enable Auto-Lock and Passcode Lock

The Auto-Lock feature makes the screen lock automatically after a specified inactivity period. Ensure that Auto-Lock is activated. The best value for Auto-lock depends on your environment:

Go to Settings > General > Auto-Lock
Set "Auto-Lock" to 3 Minutes

Enabling both Auto-Lock and Passcode Lock will ensure that the device will lock if left undisturbed. Disabling Simple Passcode enables the use of passcodes more complex than 4 numeric characters. Background discussion for balancing usability with passcode strength is provided in the *Data Protection* section of the slides available at: http://trailofbits.com/2011/08/10/ios-4-security-evaluation/

Go to Settings > General > Passcode Lock
Set "Simple Passcode" to OFF
Select "Turn Passcode On"
Set "Require Passcode" to After 1 Minute

Once a passcode is enabled, the Data Protection feature is available to apps to encrypt their data. However, only some apps, such as Mail, use the Data Protection feature to protect their data.

The Erase Data feature can be used to erase all user-created data after ten failed passcode attempts.

Go to Settings > General > Passcode Lock
Set "Erase Data" to ON

Do Not Join Untrusted Wireless Networks

When possible, avoid or limit the use of wireless networks. When not actively using wireless, turn it off to prevent any accidental exposure and conserve battery life.

Go to Settings > Wi-Fi
Set "Wi-Fi" to OFF

Resist the temptation to use free Wi-Fi access points. These typically offer no protection for wirelessly transmitted data, meaning that anyone in the vicinity could intercept all traffic transmitted or received. If it is necessary to use a WiFi network, choose a known one and ensure that its traffic is encrypted, preferably with WPA2 or WPA. Protected networks are designated in the list of available networks by a picture of a lock next to their names.

To avoid accidentally joining an untrusted network, turn off "Ask to Join Networks." This will not prevent your iOS device from reconnecting to networks it has joined in the past, but it will require future wireless connections to be made manually by selecting a network from a list.

Go to Settings > Wi-Fi
Set "Ask to Join Networks" to OFF

Note: Even if this setting is disabled, your iOS device will still automatically rejoin previously visited networks that have not been explicitly forgotten.

Another precaution is to choose "Forget this network" at the end of a wireless session. This will reduce the chance that your iOS device may accidentally join another wireless network with the same name. It is important to select this option before leaving the physical range of the network in question. Otherwise, the network will no longer appear in the list of available networks, and it will not be possible to remove it.

Go to Settings > Wi-Fi
Select a network from the list
Set "Forget this network"

Disable Bluetooth Unless Needed

Use Bluetooth only when necessary. When not in use, disable it to prevent other devices from discovering your iOS device and attempting to connect to it.

Go to Settings > General > Bluetooth
Set "Bluetooth" to OFF

Disable Location Services Unless Needed

Location Services can be used by apps or web pages on your iOS device to track your location. Unless there is some critical need for some apps to know your location, Location Services should be turned off:

Go to Settings > Location Services
Set "Location Services" to OFF

In addition, system services which provide location information to apps can be disabled when Location Services is active.

Set "Location Services" to ON
Go to System Services
Set items OFF unless needed

Individual apps that use Location Services will ask for permission to use it during their first launch. Consider these requests carefully.

Secure Safari Settings

AutoFill should be disabled in Safari, to prevent it from storing sensitive information such as usernames and passwords.

Go to Settings > Safari
Set "AutoFill" to OFF

Safari includes a fraud warning feature. This allows it to prevent browsing to fraudulent sites, which are stored on a blacklist.

Set "Fraud Warning" to ON

JavaScript support can be disabled to prevent execution of maliciously crafted JavaScripts. However, this may not be practical due to websites' frequent usage of JavaScript.

Set "JavaScript" to OFF *if practical*

Pop-ups are annoying and can also present security problems.

Set "Block Pop-ups" to ON

Cookies can compromise personal information and browsing habits. To decrease this risk, disable them or set Safari to only accept cookies from visited sites.

Set "Accept Cookies" to From visited

Secure Mail Settings

Ensure that all Mail connections are encrypted. This requires that your email server support encryption, which most do. Without encryption support, your messages will be sent in the clear, which could make it possible for someone to intercept and read them.

Go to Settings > Mail, Contacts, Calendars
For each account in the list:
Select SMTP, then select the server on the next screen
Set "Use SSL" to ON

For each account in the list:
Go to Advanced
Set "Use SSL" to ON

If accessing web mail through Safari, make sure the login page is encrypted before entering your data. If it is encrypted, the URL will start with "https" instead of "http," and a lock icon will appear to the right of the URL.

Remote image loading should be disabled in Mail. This can prevent maliciously crafted images from harming your iOS device. It will also prevent attackers from linking your network address information to your email account.

Go to Settings > Mail, Contacts, Calendars

Set "Load Remote Images" to OFF

Consider the iPhone Configuration Utility

For other settings, such as the ability to force encrypted backups, require more complex passcodes, and enable remote wipes, the iPhone Configuration Utility is a free tool that Apple provides directly through their website:

http://www.apple.com/support/iphone/enterprise/

The settings available through this tool correspond to settings that enterprises can deploy to devices through the use of MDM products. Some restrictions, such as use of the Camera or Safari, and installation or removal of apps, can also be controlled via the iPhone Configuration Utility or MDM products. These can also be applied in **Settings > General > Restrictions**, in the event that the user wishes to self-restrict or restrict the capabilities of another user.

The Information Assurance Mission at NSA

Security Tips for Personally Managed Apple iPhones and iPads

The Mitigations Group
National Security Agency
9800 Savage Road
Ft. Meade, MD 20755
http://www.nsa.gov/mitigations

Jan 2012