Security Benchmarks™
A DIVISION OF CENTER FOR INTERNET SECURITY

CIS Apple iOS 6 Benchmark

v1.0.0

Export Date 11-09-2012

The CIS Security Benchmarks division provides consensus-oriented information security products, services, tools, metrics, suggestions, and recommendations (the "SB Products") as a public service to Internet users worldwide. Downloading or using SB Products in any way signifies and confirms your acceptance of and your binding agreement to these CIS Security Benchmarks Terms of Use.

CIS SECURITY BENCHMARKS TERMS OF USE

BOTH CIS SECURITY BENCHMARKS DIVISION MEMBERS AND NON-MEMBERS MAY:

- Download, install, and use each of the SB Products on a single computer, and/or
- Print one or more copies of any SB Product that is in a .txt, .pdf, .doc, .mcw, or .rtf format, but only if each such copy is printed in its entirety and is kept intact, including without limitation the text of these CIS Security Benchmarks Terms of Use.

UNDER THE FOLLOWING TERMS AND CONDITIONS:

- **SB Products Provided As Is**. CIS is providing the SB Products "as is" and "as available" without: (1) any representations, warranties, or covenants of any kind whatsoever (including the absence of any warranty regarding: (a) the effect or lack of effect of any SB Product on the operation or the security of any network, system, software, hardware, or any component of any of them, and (b) the accuracy, utility, reliability, timeliness, or completeness of any SB Product); or (2) the responsibility to make or notify you of any corrections, updates, upgrades, or fixes.
- **Intellectual Property and Rights Reserved**. You are not acquiring any title or ownership rights in or to any SB Product, and full title and all ownership rights to the SB Products remain the exclusive property of CIS. All rights to the SB Products not expressly granted in these Terms of Use are hereby reserved.
- **Restrictions**. You acknowledge and agree that you may not: (1) decompile, dis-assemble, alter, reverse engineer, or otherwise attempt to derive the source code for any software SB Product that is not already in the form of source code; (2) distribute, redistribute, sell, rent, lease, sublicense or otherwise transfer or exploit any rights to any SB Product in any way or for any purpose; (3) post any SB Product on any website, bulletin board, ftp server, newsgroup, or other similar mechanism or device; (4) remove from or alter these CIS Security Benchmarks Terms of Use on any SB Product; (5) remove or alter any proprietary notices on any SB Product; (6) use any SB Product or any component of an SB Product with any derivative works based directly on an SB Product or any component of an SB Product; (7) use any SB Product or any component of an SB Product with other products or applications that are directly and specifically dependent on such SB Product or any component for any part of their functionality; (8) represent or claim a particular level of compliance or consistency with any SB Product; or (9) facilitate or otherwise aid other individuals or entities in violating these CIS Security Benchmarks Terms of Use.
- **Your Responsibility to Evaluate Risks**. You acknowledge and agree that: (1) no network, system, device, hardware, software, or component can be made fully secure; (2) you have the sole responsibility to evaluate the risks and benefits of the SB Products to your particular circumstances and requirements; and (3) CIS is not assuming any of the liabilities associated with your use of any or all of the SB Products.
- **CIS Liability**. You acknowledge and agree that neither CIS nor any of its employees, officers, directors, agents or other service providers has or will have any liability to you whatsoever (whether based in contract, tort, strict liability or otherwise) for any direct, indirect, incidental, consequential, or special damages that arise out of or are connected in any way with your use of any SB Product.
- **Indemnification**. You agree to indemnify, defend, and hold CIS and all of CIS's employees, officers, directors, agents and other service providers harmless from and against any liabilities, costs and expenses incurred by any of them in connection with your violation of these CIS Security Benchmarks Terms of Use.
- **Jurisdiction**. You acknowledge and agree that: (1) these CIS Security Benchmarks Terms of Use will be governed by and construed in accordance with the laws of the State of Maryland; (2) any action at law or in equity arising out of or relating to these CIS Security Benchmarks Terms of Use shall be filed only in the courts located in the State of Maryland; and (3) you hereby consent and submit to the personal jurisdiction of such courts for the purposes of litigating any such action.
- **U.S. Export Control and Sanctions laws**. Regarding your use of the SB Products with any non-U.S. entity or country, you acknowledge that it is your responsibility to understand and abide by all U.S. sanctions and export control laws as set from time to time by the U.S. Bureau of Industry and Security (BIS) and the U.S. Office of Foreign Assets Control (OFAC).

SPECIAL RULES FOR CIS MEMBER ORGANIZATIONS: CIS reserves the right to create special rules for: (1) CIS Members; and (2) Non-Member organizations and individuals with which CIS has a written contractual relationship. CIS hereby grants to each CIS Member Organization in good standing the right to distribute the SB Products within such Member's own organization, whether by manual or electronic means. Each such Member Organization acknowledges and agrees that the foregoing grants in this paragraph are subject to the terms of such Member's membership arrangement with CIS and may, therefore, be modified or terminated by CIS at any time.

Table of Contents

Overview

This document, *Security Configuration Benchmark for Apple iOS 5*, provides prescriptive guidance for establishing a secure configuration posture for the Apple iOS version 5.0.1. This guide was tested against the Apple iOS 5.0.1 and the iPhone Configuration Utility (iPCU) v3.4.0.283. This benchmark covers the Apple iOS 5.0.1 and all hardware devices on which this iOS is supported. As of the publication of this guidance, mobile devices supported by iOS 5.0.1 include the following:

- iPhone 4S
- iPhone 4
- iPhone 3GS
- iPhone 3
- iPad 2
- iPad
- iPod Touch (4th Generation)
- iPod Touch (3rd Generation)

In determining recommendations, the current guidance treats all iOS mobile device platforms as having the same use cases and risk/threat scenarios. In all but a very few cases, configuration steps, default settings, and benchmark recommended settings are identical regardless of hardware platform; for the few cases where variation exists, the benchmark notes the difference within the respective section. To obtain the latest version of this guide, please visit http://benchmarks.cisecurity.org. If you have questions, comments, or have identified ways to improve this guide, please write us at feedback@cisecurity.org.

Intended Audience

This document is intended for system and application administrators, security specialists, auditors, help desk, end users, and platform deployment personnel who plan to use, develop, deploy, assess, or secure solutions that incorporate the Apple iOS 5.0.1.

Consensus Guidance

This benchmark was created using a consensus review process comprised of volunteer and contract subject matter experts. Consensus participants provide perspective from a diverse set of backgrounds including consulting, software development, audit and compliance, security research, operations, government, and legal.

Each CIS benchmark undergoes two phases of consensus review. The first phase occurs during initial benchmark development. During this phase, subject matter experts convene to discuss, create, and test working drafts of the benchmark. This discussion occurs until consensus has been reached on benchmark recommendations. The second phase begins after the benchmark has been released to the public Internet. During this phase, all feedback provided by the Internet community is reviewed by the consensus team for incorporation in the benchmark. If you are interested in participating in the consensus review process, please send us a note to feedback@cisecurity.org.

Typographical Conventions

The following typographical conventions are used throughout this guide:

Convention	Meaning
`Stylized Monospace font`	Used for blocks of code, command, and script examples. Text should be interpreted exactly as presented.
`Monospace font`	Used for inline code, commands, or examples. Text should be interpreted exactly as presented.
<italic font in brackets>	Italic texts set in angle brackets denote a variable requiring substitution for a real value.
Italic font	Used to denote the title of a book, article, or other publication.
Note	Additional information or caveats

Scoring Information

A scoring status indicates whether compliance with the given recommendation impacts the assessed target's benchmark score. The following scoring statuses are used in this benchmark:

Scored
Failure to comply with "Scored" recommendations will decrease the final benchmark score. Compliance with "Scored" recommendations will increase the final benchmark score.

Not Scored
Failure to comply with "Not Scored" recommendations will not decrease the final benchmark score. Compliance with "Not Scored" recommendations will not increase the final benchmark score.

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **Level 1 - Apple iOS 5**

  Items in this profile intend to:

  - be practical and prudent;
  - provide a clear security benefit; and
  - not negatively inhibit the utility of the technology beyond acceptable means.
- **Level 2 - Apple iOS 5**

  This profile extends the "Level 1" profile. Items in this profile exhibit one or more of the following characteristics:

  - are intended for environments or use cases where security is paramount.
  - acts as defense in depth measure.
  - may negatively inhibit the utility or performance of the technology.
- **Level 1 - Apple iOS 4**

  Items in this profile intend to:

  - be practical and prudent;
  - provide a clear security benefit; and
  - not negatively inhibit the utility of the technology beyond acceptable means.
- **Level 2 - Apple iOS 4**

  This profile extends the "Level 1" profile. Items in this profile exhibit one or more of the following characteristics:

  - are intended for environments or use cases where security is paramount.
  - acts as defense in depth measure.
  - may negatively inhibit the utility or performance of the technology.
- **Level 1 - Apple iOS 6**

  Items in this profile intend to:

  - be practical and prudent;
  - provide a clear security benefit; and
  - not negatively inhibit the utility of the technology beyond acceptable means.
- **Level 2 - Apple iOS 6**

This profile extends the "Level 1" profile. Items in this profile exhibit one or more of the following characteristics:

- are intended for environments or use cases where security is paramount.
- acts as defense in depth measure.
- may negatively inhibit the utility or performance of the technology.

Acknowledgements

This benchmark exemplifies the great things a community of users, vendors, and subject matter experts can accomplish through consensus collaboration. The CIS community thanks the entire consensus team with special recognition to the following individuals who contributed greatly to the creation of this guide:

Author
David Skrdla

Contributor
Blake Frantz , *Center for Internet Security*
Brian Reilly
Joe Wulf RHCSA(RHEL6), FITSP-D, CISSP, VCP3, CPO (USN RET), *U.S. National Security Agency*
Rebecca Heffel
Richard Tychansky
Roland Grefer
Shawn Geddis
Toon Mordijck
Richard Haas
Adrian Sanabria

Editor
David Skrdla
Mike de Libero

TBD

TBD

Recommendations

1 User Interface Settings

This section provides guidance on the secure configuration of iOS mobile devices using the device user interface.

1.1 System Settings

This section provides guidance on the secure configuration of system settings.

1.1.1 Update firmware to latest version (Not Scored)

Profile Applicability:

- Level 1 - Apple iOS 5
- Level 2 - Apple iOS 5

Description:

This control ensures that the device firmware remains current.

Rationale:

Firmware updates often include critical security fixes that reduce the probability of an attacker exploiting the device.

Audit:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `About`.
4. Confirm that "Version" is 6.0.1.

Remediation:

Using iTunes:

1. Connect the device to the computer.
2. Open iTunes.
3. Click on the device under "Devices" in the source list.

4. Click on `Check for Update`.
5. Click `Download and Install`.
6. Do not disconnect the device until the update is finished.

Using Over-the-Air Update:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `Software Update`.
4. iOS will automatically check for available updates. If an update is available, tap `Download` when prompted to download the update.
5. Once the download has completed, tap `Install` to update the iOS.
6. Do not power off the device until the update is finished.

References:

1. iOS: How to update your iPhone, iPad, or iPod touch. Available: http://support.apple.com/kb/HT4623
2. iOS 5: Updating your device to iOS 5. Available: http://support.apple.com/kb/HT4972
3. iOS: How to back up. Available: http://support.apple.com/kb/HT1766

1.1.2 Require Passcode on Device (Not Scored)

Profile Applicability:

- Level 1 - Apple iOS 5
- Level 2 - Apple iOS 5

Description:

This control determines whether a password is required before allowing access to the device via the touch screen.

Rationale:

Requiring a password to unlock the device helps prevent unauthorized access to the device and increases the effort required to use the device or access data stored on it.

Audit:

1. Tap `Settings`.
2. Tap `General`.
3. Confirm that Passcode Lock is turned on.

Remediation:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `Passcode Lock`.
4. Tap `Turn Passcode On`.
5. Tap in a passcode.
6. Tap in the same passcode.

1.1.3 Configure an alphanumeric value (Not Scored)

Profile Applicability:

- Level 2 - Apple iOS 5

Description:

This control determines whether alphanumeric characters (alphabetic and non-alphanumeric values in addition to numerals) are permitted for the passcode protecting access to the device via the touch screen.

Rationale:

Permitting an alphanumeric password to be configured to unlock the device permits the user to increase the difficulty of determining the password by an attacker seeking unauthorized access.

Audit:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `Passcode Lock`.
4. Enter current passcode as prompted.
5. Confirm that Simple Passcode is turned off.

Remediation:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `Passcode Lock`.
4. Enter current passcode if configured.
5. Turn off Simple Passcode.
6. Enter previous password when prompted.
7. Enter new complex passcode twice as prompted.

1.1.4 Set auto-lock timeout (Not Scored)

Profile Applicability:

- Level 1 - Apple iOS 5
- Level 2 - Apple iOS 5

Description:

This control defines the number of minutes the device can be inactive before requiring the password be reentered.

Rationale:

Automatically locking the device after a short period of inactivity reduces the probability of an attacker accessing the device without entering a password.

Audit:

1. Tap `Settings`.
2. Tap `General`.
3. Review the Auto-lock interval:
   a) For typical use cases, confirm that the Auto-Lock is set to `5 minutes or less`.
   b) For high-security use cases, confirm that Auto-Lock is set to `2 minutes`.

Remediation:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `Auto-Lock`.
4. Set the Auto-lock interval:
   a) For typical use cases, tap `5 Minutes` or less.
   b) For high-security use cases, tap `2 Minutes`.

1.1.5 Erase data upon excessive passcode failures (Not Scored)

Profile Applicability:

- Level 1 - Apple iOS 5
- Level 2 - Apple iOS 5

Description:

This setting determines how many failed passcode attempts can be made before the device is wiped.

Rationale:

Excessive passcode failures typically indicate that the device is out of physical control of its owner. Upon such an event, erasing data on the phone will help to ensure the confidentiality of information stored on the device is protected when facing a novice attacker.

Audit:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `Passcode Lock`.
4. Enter current passcode as prompted.
5. Confirm that Erase Data is turned on.

Remediation:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `Passcode Lock`.
4. Enter current passcode as prompted.
5. Turn on Erase Data.
6. Tap `Enable` on confirmation dialog.

1.1.6 Forget Wi-Fi networks to prevent automatic rejoin (Not Scored)

Profile Applicability:

- Level 2 - Apple iOS 5

Description:

This configuration causes an iOS device to forget Wi-Fi networks with which it has previously associated.

Rationale:

A trusted but unauthenticated Wi-Fi network may be spoofed and automatically joined if it is not forgotten after last use. Additionally, if such a network has a common SSID, such as "default" or "linksys", it is probable that the iOS device will encounter an untrusted instance of a same-named Wi-Fi network and automatically attempt to join it.

Audit:

1. Tap `Settings`.

2. Tap `Wi-Fi`.
3. From the Choose a Network list, locate the network SSID and tap the chevron next to the Wi-Fi network to check.
4. Confirm that the network configuration does not have the "Forget this network" option available.

Remediation:

1. Tap `Settings`.
2. Tap `Wi-Fi`.
3. From the Choose a Network list, locate the network SSID and tap the chevron next to the Wi-Fi network you want to forget (see note below).
4. Tap `Forget this network`.
5. Tap `Forget` on the confirmation dialog.

Note: Wi-Fi must be turned on and the Wi-Fi network must be in range for it to appear in the list of available networks to configure. The Wi-Fi network must be remembered or currently connected for the "Forget this network" option to be present. If the Wi-Fi network is no longer in range, the user will not be able to selectively forget it, but instead must reset all network settings to forget all Wi-Fi networks.

1.1.7 Turn off Ask to Join Networks (Not Scored)

Profile Applicability:

- Level 2 - Apple iOS 5

Description:

When the device is trying to access the Internet and is not in range of a Wi-Fi network it has previously used, this option tells the device to look for another network and display a list of all available Wi-Fi networks that the user can choose from. If "Ask to Join Networks" is turned off, the user must manually search for a network to connect to.

Rationale:

Requiring the user to manually configure and join a Wi-Fi network reduces the risk of inadvertently joining a similarly named yet untrusted network (i.e. "default" vice "defualt").

Audit:

1. Tap `Settings`.
2. Tap `Wi-Fi`.

3. Confirm that Ask to Join Networks is turned off.

Remediation:

1. Tap `Settings`.
2. Tap `Wi-Fi`.
3. Turn off Ask to Join Networks (see note below).

Note: Wi-Fi must be turned on for the above Wi -Fi configuration option to appear.

1.1.8 Turn off Auto-Join for all Wi-Fi networks (Not Scored)

Profile Applicability:

- Level 2 - Apple iOS 5

Description:

When Wi-Fi Auto-Join is turned on for a Wi-Fi network, the device remembers the network and login information and automatically reconnects to that Wi-Fi network whenever the device is in range.

Rationale:

Auto-Join may expose credentials at unexpected times and locations (e.g., if forms-based authentication occurs over unencrypted HTTP, or a spoofed SSID is encountered), and for Wi-Fi networks that require HTTP(S) forms authentication, this feature will cause credentials to persist on disk, potentially placing the the confidentiality of the credentials at risk if physical custody of the device is lost.

Audit:

1. Tap `Settings`.
2. Tap `Wi-Fi`.
3. From the Choose a Network list, locate the network SSID and tap the chevron next to the network to review.
4. Confirm that Auto-Join is turned off.
5. Repeat steps 3 and 4 for each network SSID.

Remediation:

1. Tap `Settings`.
2. Tap `Wi-Fi`.

3. From the Choose a Network list, locate the network SSID and tap the chevron next to the network to change.
4. Turn off Auto-Join (see note below).
5. Repeat steps 3 and 4 for each network SSID.

Note: Wi-Fi must be turned on and the Wi-Fi network must be in range for it to appear in the list of available networks to configure. The Wi-Fi network must require network login credentials and must be remembered or currently connected for the Auto-Join option to be present.

References:

1. iPhone, iPad, iPod touch: Understanding subscription Wi-Fi networks. Available: http://support.apple.com/kb/HT3867

1.1.9 Turn off Wi-Fi when not needed (Not Scored)

Profile Applicability:

- Level 2 - Apple iOS 5

Description:

This setting determines whether the iOS device uses local Wi-Fi networks to connect to the Internet and other networks.

Rationale:

Disabling the Wi-Fi interface reduces the remote attack surface of the device.

Audit:

1. Tap `Settings`.
2. Tap `Wi-Fi`.
3. Confirm that Wi-Fi is turned off.

Remediation:

1. Tap `Settings`.
2. Tap `Wi-Fi`.
3. Turn off Wi-Fi.

1.1.10 Turn off VPN when not needed (Not Scored)

Profile Applicability:

- Level 1 - Apple iOS 5
- Level 2 - Apple iOS 5

Description:

iOS devices can connect to VPNs that use the L2TP, PPTP, or Cisco IPSec protocols. VPN connections can be established over both Wi-Fi and cellular data network connections.

Rationale:

If the device has a VPN connection configured, it should only be turned on when VPN access is required. If the VPN is left on, the user may not be mindful of the nature of the information they are transmitting on the network. Additionally, malicious or exploited iPhone applications may access VPN resources.

Audit:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `Network`.
4. Tap `VPN`.
5. Confirm that VPN is turned off.

Remediation:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `Network`.
4. Tap `VPN`.
5. Turn off VPN if turned on.

1.1.11 Turn off Bluetooth when not needed (Not Scored)

Profile Applicability:

- Level 1 - Apple iOS 5
- Level 2 - Apple iOS 5

Description:

Bluetooth allows devices to connect wirelessly to headsets, car kits, and other accessories for various Bluetooth profile functionality.

Rationale:

Disabling Bluetooth when not needed reduces the remote attack surface of the device and prevents discovery of and connection to Bluetooth services.

Audit:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `Bluetooth`.
4. Confirm that Bluetooth is turned off.

Remediation:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `Bluetooth`.
4. Turn off Bluetooth.

1.1.12 Turn off Personal Hotspot when not needed (Not Scored)

Profile Applicability:

- Level 2 - Apple iOS 5

Description:

iOS 6 devices with cellular data connections can be configured to share an active Cellular Data connection using Personal Hotspot via Wi-Fi (iPhone 4), Bluetooth, or USB.

Rationale:

Disabling the Personal Hotspot makes the hotspot unavailable to unauthorized access attempts and reduces the overall remote attack surface of the device.

Audit:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `Network`.
4. Tap `Personal Hotspot`.
5. Confirm that Personal Hotspot is turned off.

Remediation:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `Network`.
4. Tap `Personal Hotspot`.
5. Turn off Personal Hotspot.

1.1.13 Turn off Location Services (Not Scored)

Profile Applicability:

- Level 2 - Apple iOS 5

Description:

Location Services allows applications such as Maps, Internet, and Camera to gather and use data indicating the user's location. The user's approximate location is determined using available information from cellular network data, local Wi-Fi networks (if the user has Wi-Fi turned on), and GPS as available.

Rationale:

Disabling location services reduces the capability of an attacker to determine or track the user's location via websites, locally installed applications or other means.

Audit:

1. Tap `Settings`.
2. Tap `Location Services`.
3. Confirm that Location Services is turned off.

Remediation:

1. Tap `Settings`.
2. Tap `Location Services`.
3. Turn off Location Services.

Note: Location services can also be disabled/enabled on a per-app basis within the Locations Services configuration menu referenced above.

1.1.14 Turn on Airplane Mode (Not Scored)

Profile Applicability:

- Level 2 - Apple iOS 5

Description:

Airplane Mode disables all receivers and transceivers on a mobile device. When Airplane Mode is on, no cellular voice, cellular data, GPS, radio, Wi-Fi, or Bluetooth signals are emitted from or received by the device.

Rationale:

If the user enters an environment where no signal transmission or reception is intended, Airplane Mode can be turned on to ensure that the device does not initiate or respond to any signals. This reduces the remote attack surface.

Audit:

1. Tap `Settings`.
2. Confirm that Airplane Mode is on.

Remediation:

1. Tap `Settings`.
2. Turn on Airplane Mode.

1.1.15 Erase all data before return, recycle, reassignment, or other disposition (Not Scored)

Profile Applicability:

- Level 1 - Apple iOS 5
- Level 2 - Apple iOS 5

Description:

This control effectively erases all data, including accounts, from the device's internal storage by securely discarding the block storage encryption key from Effaceable Storage, rendering all data unreadable.

Rationale:

In normal operations, deleting data on an iOS device renders it inaccessible through the user interface but the data is not erased from the device. Erasing stored data by securely discarding the block storage encryption key before returning, recycling, disposing of, or otherwise placing a device out of the user's control reduces the probability of an attacker subsequently accessing confidential information previously stored on the device.

Audit:

To verify that the iPhone disk has been overwritten, it is necessary to install a warranty-voiding forensics recovery toolkit that is not within the scope of this document. Please review the reference for more information.

Remediation:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `Reset`.
4. Tap `Erase All Contents and Settings`.
5. If passcode is configured on device, enter passcode when prompted.

References:

1. iPhone Forensics. Available: http://oreilly.com/catalog/9780596153588/

1.1.16 Disable View in Lock Screen for apps when device is locked (Not Scored)

Profile Applicability:

- Level 2 - Apple iOS 5

Description:

This setting prevents notifications from any source from being displayed when the iOS device is passcode locked.

Rationale:

Parties who do not know the passcode lock should not have read access to the notifications displayed by the device.

Audit:

1. Tap `Settings`.
2. Tap `Notifications`.
3. From the list of notification sources listed in the Notifications panel, locate the app or other notification source and tap the chevron next to the source to review.
4. Confirm that View in Lock Screen is turned off.
5. Repeat steps 3 and 4 for each source.

Remediation:

1. Tap `Settings`.
2. Tap `Notifications`.
3. From the list of notification sources listed in the Notifications panel, locate the app or other notification source and tap the chevron next to the source to change.
4. Turn off "View in Lock Screen".
5. Repeat steps 3 and 4 for each source.

1.2 Safari Settings

This section provides guidance on the secure configuration of settings related to the Safari application on the iOS mobile devices.

1.2.1 Disable JavaScript (Not Scored)

Profile Applicability:

- Level 2 - Apple iOS 5

Description:

JavaScript lets web programmers control elements of the page—for example, a page that uses JavaScript might display the current date and time or cause a linked page to appear in a new pop-up page. It is recommended that JavaScript be disabled in environments where security is paramount.

Rationale:

JavaScript should only be enabled before browsing trusted sites.

Audit:

1. Tap `Settings`.
2. Tap `Safari`.
3. Confirm that JavaScript is turned off.

Remediation:

1. Tap `Settings`.
2. Tap `Safari`.
3. Turn off JavaScript.

1.2.2 Enable Fraud Warning (Not Scored)

Profile Applicability:

- Level 1 - Apple iOS 5
- Level 2 - Apple iOS 5

Description:

Fraud warning protects you from potentially fraudulent Internet sites. When you visit a suspicious site, Safari warns you about its suspect nature and doesn't load the page. It is recommended that the Fraud Warning feature be enabled.

Rationale:

Enabling a warning can help you avoid accidently visiting some known phishing and other fraudulent sites covered by this feature.

Audit:

1. Tap `Settings`.
2. Tap `Safari`.
3. Confirm that Fraud Warning is turned on.

Remediation:

1. Tap `Settings`.
2. Tap `Safari`.
3. Turn on Fraud Warning.

1.2.3 Disable Auto Fill (Not Scored)

Profile Applicability:

- Level 2 - Apple iOS 5

Description:

The browser has a feature to remember information entered into common forms in order to automate the completion of later forms. Information auto-filled can include information from Contacts as well as remembered names and passwords.

- If Use Contact Info is turned on and contact information selected, Safari will use the selected information from Contacts to fill in contact fields on web forms.
- If Names & Passwords is turned on, Safari will remember names and passwords to websites visited and automatically fill in the information when you revisit the website.

Rationale:

Disabling AutoFill can help avoid the storage of credentials locally on the device, as well as reduces the likelihood of automated unauthorized access to a site in the event unauthorized access is gained to the device.

Audit:

1. Tap `Settings`.
2. Tap `Safari`.
3. Tap `AutoFill`.
4. Confirm that AutoFill is turned off for the "Use Contact Info" setting.
5. Confirm that AutoFill is turned off for the "Names and Passwords" setting.

Remediation:

1. Tap `Settings`.
2. Tap `Safari`.
3. Tap `AutoFill`.
4. Turn off "Use Contact Info"
5. Turn off "Names and Passwords".

1.2.4 Turn On Private Browsing When Needed (Not Scored)

Profile Applicability:

- Level 2 - Apple iOS 5

Description:

The Safari browser on iOS devices keeps a history of web pages visited, searches performed, and (if configured) certain AutoFill information. The tracking of this information can be prevented for a browser session by enabling Private Browsing. When enabled, Safari bars will appear black or dark instead of blue or gray.

The Private Browsing option may not prevent Safari from collecting cookies from all websites. To more robustly reduce the ability of websites or local users to track activity, also ensure that the Accept Cookies option is turned off.

Rationale:

Enabling Private Browsing can protect certain private information and block some websites from tracking browser activity; enabled, Safari will not remember web pages visited, search history, or AutoFill information used within the Private Browsing session.

Audit:

1. Tap `Settings`.
2. Tap `Safari`.
3. Confirm that Private Browsing is turned off.

Remediation:

1. Tap `Settings`.
2. Tap `Safari`.
3. Turn off Private Browsing.

References:

1. iOS: Safari web settings. Available: http://support.apple.com/kb/HT1677

2 iPhone Configuration Utility Settings

This section provides guidance on the secure configuration of iOS mobile devices with the iPhone Configuration Utility (iPCU), version 3.4.0.283. The iPhone Configuration Utility is a download available from Apple at http://www.apple.com/support/iphone/enterprise that lets users create, maintain, and sign configuration profiles, track and install provisioning profiles and authorized applications, and capture device information including console logs.

2.1 System Settings

This section provides guidance on the secure configuration of system settings.

2.1.1 Disallow profile removal (Scored)

Profile Applicability:

- Level 1 - Apple iOS 5
- Level 2 - Apple iOS 5

Description:

The device can be configured to always allow the removal of a profile, to allow the removal of a profile only with a profile-specific password, or to never allow the removal of a profile,

on a per-profile basis. By default, the iPCU configuration allows the profile to be removed by the user. To ensure profile settings remain in effect, profile removal must be disallowed.

Rationale:

Restricting the removal of a configuration profile is necessary to enforce the settings contained within the respective profile. If a user can circumvent profile requirements simply by uninstalling the profile, the continued enforcement of profile controls cannot be assured and intended device security is highly reduced.

Audit:

1. Open the configuration profile XML file.
2. Search for `<key>PayloadRemovalDisallowed</key>`.
3. Observe if the next line is `<true/>`.
4. Search for `<key>RemovalPassword</key>`.
5. Observe whether this value is present and whether a value is set.

Remediation:

1. Open iPCU.
2. Click on `Configuration Profiles` in the left windowpane.
3. Click on the `General` tab in the lower right windowpane.
4. Click on the `Security` combo box in the lower right window pane.
5. Select `With Authentication`.
6. Install the configuration profile on the device.

2.2 Passcode Settings

This section provides guidance on the secure configuration of passcode settings.

2.2.1 Require passcode on device (Scored)

Profile Applicability:

- Level 1 - Apple iOS 5
- Level 2 - Apple iOS 5

Description:

This control determines whether a password is required before allowing access to the device via the touch screen.

Rationale:

Requiring a password to unlock the device helps prevent unauthorized access to the device and increases the effort required to use the device or access data stored on it.

Audit:

1. Open the configuration profile XML file.
2. Search for `<key>forcePIN</key>`.
3. Observe if the next line is `<true/>`.

Remediation:

1. Open iPCU.
2. Click on `Configuration Profiles` in the left windowpane.
3. Click on the `Passcode` tab in the lower right windowpane.
4. If a passcode is not currently required, you will be prompted to Configure Passcode Policy. Click on the `Configure` button in the prompt.
5. Install the configuration profile on the device.

2.2.2 Require alphanumeric value (Scored)

Profile Applicability:

- Level 2 - Apple iOS 5

Description:

This control determines whether alphanumeric characters (alphabetic and non-alphanumeric values in addition to numerals) are required for the passcode that protects access to the device via the touch screen.

Rationale:

Requiring a mix of alphabetical and numerical characters increases the complexity of the passcode and therefore the the difficulty of determining the password by an attacker seeking unauthorized access.

Audit:

1. Open the configuration profile XML file.
2. Search for `<key>requireAlphanumeric</key>`.
3. Observe if the next line is `<true/>`.

Remediation:

1. Open iPCU.

2. Click on `Configuration Profiles` in the left windowpane.
3. Click on the `Passcode` tab in the lower right windowpane.
4. Click on the `Require alphanumeric value` checkbox in the lower right windowpane.
5. Install the configuration profile on the device.

2.2.3 Set minimum passcode length (Scored)

Profile Applicability:

- Level 1 - Apple iOS 5
- Level 2 - Apple iOS 5

Description:

This control specifies the minimum number of characters a passcode can contain. It is recommended that passcode length be at least five (5) characters.

Rationale:

Requiring at least five characters increases the complexity of the passcode an attacker may attempt to brute-force in order to gain access to the device.

Audit:

1. Open the configuration profile XML file.
2. Search for `<key>minLength</key>`.
3. Observe if the next line is `<integer>5</integer>`.

Remediation:

1. Open iPCU.
2. Click on `Configuration Profiles` in the left windowpane.
3. Click on the `Passcode` tab in the lower right windowpane.
4. Click on the `Minimum passcode length` textbox in the lower right windowpane.
5. Enter the number "5".
6. Install the configuration profile on the device.

2.2.4 Set a minimum number of complex characters (Scored)

Profile Applicability:

- Level 2 - Apple iOS 5

Description:

This setting specifies the minimum number of non-alphanumeric characters (such as $, &, and !) that the passcode must contain. It is recommended that at least one non-alphanumeric character be used in the passcode.

Rationale:

Requiring at least one complex character increases the complexity of the passcode an attacker may attempt to brute-force in order to gain access to the device.

Audit:

1. Open the configuration profile XML file.
2. Search for `<key>minComplexChars</key>`.
3. Observe if the next line is `<integer>1</integer>`.

Remediation:

1. Open iPCU.
2. Click on `Configuration Profiles` in the left windowpane.
3. Click on the `Passcode` tab in the lower right windowpane.
4. Click on the `Minimum number of complex characters` textbox in the lower right windowpane.
5. Enter the number "1".
6. Install the configuration profile on the device.

References:

1. NIST SP800-63-1, Electronic Authentication Guideline - Revision 1. Available: http://csrc.nist.gov/publications/nistpubs/800-63-1/SP-800-63-1.pdf

2.2.5 Set auto-lock timeout (Scored)

Profile Applicability:

- Level 1 - Apple iOS 5
- Level 2 - Apple iOS 5

Description:

This control defines the number of minutes the device can be inactive before requiring the password be reentered. It is recommended that an inactivity timeout of no more than five (5) minutes be set for typical use cases and no more than two (2) minutes for high-security use cases.

Rationale:

Automatically locking the device after a short period of inactivity reduces the probability of an attacker accessing the device without entering a password.

Audit:

1. Open the configuration profile XML file.
2. Search for `<key>maxInactivity</key>`.
3. Review the configured Auto-lock interval:
   a) For typical use cases, observe if the next line is `<integer>5</integer>`.
   b) For high-security use cases, observe if the next line is `<integer>2</integer>`.

Remediation:

1. Open iPCU.
2. Click on `Configuration Profiles` in the left windowpane.
3. Click on the `Passcode` tab in the lower right windowpane.
4. Click on the `Auto-lock (in minutes)` drop-down menu in the lower right windowpane.
5. Set the Auto-lock interval:
   a) For typical use cases, select the number `5`.
   b) For high-security use cases, select the number `2`.
6. Install the configuration profile on the device.

2.2.6 Erase data upon excessive passcode failures (Scored)

Profile Applicability:

- Level 1 - Apple iOS 5
- Level 2 - Apple iOS 5

Description:

This setting determines how many failed passcode attempts can be made before the device is wiped (configurable from 4 to 10).

Rationale:

Excessive passcode failures typically indicate that the device is out of physical control of its owner. Upon such an event, erasing data on the phone will help to ensure the confidentiality of information stored on the device is protected when facing a novice attacker.

Audit:

1. Open the configuration profile XML file.

2. Search for `<key>maxFailedAttempts</key>`.
3. Observe if the next line is `<integer>6</integer>`.

Remediation:

1. Open iPCU.
2. Click on `Configuration Profiles` in the left windowpane.
3. Click on the `Passcode` tab in the lower right windowpane.
4. Click on the `Maximum number of failed attempts` combo box in the lower right windowpane.
5. Select the number `6`.
6. Install the configuration profile on the device.

3 Microsoft Exchange ActiveSync Policy Settings

This section provides guidance on the configuration of certain policies on iOS mobile devices using Microsoft Exchange ActiveSync versions 2.5 and later. This guidance was developed and tested specifically with Exchange ActiveSync version 3.5 with the Client Access server role on Microsoft Exchange Server 2010.

3.1 Passcode Settings

This section provides guidance on the secure configuration of passcode settings.

3.1.1 Require passcode on device (Scored)

Profile Applicability:

- Level 1 - Apple iOS 5
- Level 2 - Apple iOS 5

Description:

The device can be configured to require a passcode before allowing access through the touchpad. By default, iOS devices do not require a passcode to unlock the device after a period of inactivity, and the default Exchange ActiveSync policy setting applied for users not assigned to a mailbox policy does not require a passcode. It is recommended that a passcode be set.

Rationale:

Requiring a passcode to unlock the device increases the effort required to compromise the features and data of the iPhone in the event of a physical security breach.

Audit:

Using the Exchange Management Console (EMC):

In the "Properties" configuration window,

1. Click on the `Password` tab.
2. Observe if the `Require passcode` checkbox is selected.
3. Click `Cancel`.

Using the Exchange Management Shell:

At the Exchange Management Shell command prompt,

1. Enter the following command (all one line):

```
Get-ActiveSyncMailboxPolicy -Identity "<PolicyName>"
```

   where *<PolicyName>* is the name of the Exchange ActiveSync mailbox policy for which the audit validation should be made (replace brackets and text with appropriate policy name).

2. Search the outputted policy setting list for the "DevicePasswordEnabled :" configuration item.
3. Observe if the value following the colon is "True" as shown below

```
DevicePasswordEnabled : True
```

4. Exit the Exchange Management Shell.

Remediation:

Using the Exchange Management Console (EMC):

In the "Properties" configuration window,

1. Click on the `Password` tab.
2. Click on the `Require passcode` checkbox.
3. Click `OK`.

Using the Exchange Management Shell:

At the Exchange Management Shell command prompt,

1. Enter the following command (all one line):

```
Set-ActiveSyncMailboxPolicy -Identity "<PolicyName>"
-DevicePasswordEnabled: $true
```

where *<PolicyName>* is the name of the Exchange ActiveSync mailbox policy for which the configuration should be made (replace brackets and text with appropriate policy name).

3.1.2 Require alphanumeric value (Scored)

Profile Applicability:

- Level 2 - Apple iOS 5

Description:

The device can be configured to require that the passcode be comprised of both numeric and alphabetic values. By default, iOS devices do not enforce a passcode complexity policy, and the default Exchange ActiveSync policy setting applied for users not assigned to a mailbox policy does not require an alphanumeric passcode. It is recommended that both numeric and alphabetic values comprise the passcode.

Rationale:

Requiring a mix of alphabetical and numerical characters increases the complexity of the passcode an attacker may attempt to brute-force in order to gain access to the device.

Audit:

Using the Exchange Management Console (EMC):

In the "Properties" configuration window,

1. Click on the `Password` tab.
2. Observe if the "`Require alphanumeric passcode`" checkbox is selected.
3. Click `Cancel`.

Using the Exchange Management Shell:

At the Exchange Management Shell command prompt,

1. Enter the following command (all one line):

```
Get-ActiveSyncMailboxPolicy -Identity "<PolicyName>"
```

where <*PolicyName*> is the name of the Exchange ActiveSync mailbox policy for which the audit validation should be made (replace brackets and text with appropriate policy name).

2. Search the outputted policy setting list for the "AlphanumericDevicePasswordRequired :" configuration item.
3. Observe if the value following the colon is "True" as shown below:
   `AlphanumericDevicePasswordRequired : True`
4. Exit the Exchange Management Shell.

Remediation:

Using the Exchange Management Console (EMC):

In the "Properties" configuration window,

1. Click on the `Password` tab.
2. Click on the `Require alphanumeric passcode` checkbox.
3. Click `OK`.

Using the Exchange Management Shell:

At the Exchange Management Shell command prompt,

1. Enter the following command (all one line):

```
Set-ActiveSyncMailboxPolicy -Identity "<PolicyName>"
 -AlphanumericDevicePasswordRequired : $true
```

where <*PolicyName*> is the name of the Exchange ActiveSync mailbox policy for which the configuration should be made (replace brackets and text with appropriate policy name).

3.1.3 Set minimum passcode length (Scored)

Profile Applicability:

- Level 1 - Apple iOS 5
- Level 2 - Apple iOS 5

Description:

The device can be configured to require that the passcode be at least a pre-determined length. By default, the minimum passcode length is only four characters, and this is the

default Exchange ActiveSync policy value applied for users not assigned to a mailbox policy if minimum password length checking is enabled. It is recommended that password length be at least five (5) characters.

Rationale:

Requiring at least five characters increases the complexity of the passcode an attacker may attempt to brute-force in order to gain access to the device. Additionally, requiring at least five characters prevents a user from selecting typically weak values, such as a year, date, or last four digits of a phone number, for their passcode.

Audit:

Using the Exchange Management Console (EMC):

In the "Properties" configuration window,

1. Click on the `Password` tab.
2. Observe if the "Minimum password length" checkbox is selected.
3. Observe if the minimum password length value is set to 5.
4. Click `Cancel`.

Using the Exchange Management Shell:

At the Exchange Management Shell command prompt,

1. Enter the following command (all one line):

```
Get-ActiveSyncMailboxPolicy -Identity "<PolicyName>"
```

   where *<PolicyName>* is the name of the Exchange ActiveSync mailbox policy for which the audit validation should be made (replace brackets and text with appropriate policy name).

2. Search the outputted policy setting list for the "MinDevicePasswordLength :" configuration item.
3. Observe if there is a value following the colon and that the value is set to 5 as shown below:

```
MinDevicePasswordLength : 5
```

4. Exit the Exchange Management Shell.

Remediation:

Using the Exchange Management Console (EMC):

In the "Properties" configuration window,

1. Click on the `Password` tab.
2. Click on the `Minimum password length` checkbox.
3. Enter the number 5 in the box on the right hand side.
4. Click `OK`.

Using the Exchange Management Shell:

At the Exchange Management Shell command prompt,

1. Enter the following command (all one line):

```
Set-ActiveSyncMailboxPolicy -Identity "<PolicyName>" -MinDevicePasswordLength 5
```

   where *<PolicyName>* is the name of the Exchange ActiveSync mailbox policy for which the configuration should be made (replace brackets and text with appropriate policy name).

3.1.4 Set a minimum number of complex characters (Scored)

Profile Applicability:

- Level 2 - Apple iOS 5

Description:

The device can be configured to require non-alphanumeric characters in the passcode. By default, iOS devices do not require complex characters in the passcode, and the default minimum value Exchange ActiveSync policy applies for users not assigned to a mailbox policy is zero (0). It is recommended that a non-alphanumeric character be used in the passcode.

Rationale:

Requiring at least one complex character increases the complexity of the passcode an attacker may attempt to brute-force in order to gain access to the device.

Audit:

Using the Exchange Management Console (EMC):

In the "Properties" configuration window,

1. Click on the `Password` tab.
2. Observe if the "Require alphanumeric passcode" checkbox is selected.
3. Observe if the "Minimum number of complex characters" value is set to 1.
4. Click `Cancel`.

Using the Exchange Management Shell:

At the Exchange Management Shell command prompt,

1. Enter the following command (all one line):

```
Get-ActiveSyncMailboxPolicy -Identity "<PolicyName>"
```

   where *<PolicyName>* is the name of the Exchange ActiveSync mailbox policy for which the audit validation should be made (replace brackets and text with appropriate policy name).

2. Search the outputted policy setting list for the "MinDevicePasswordComplexCharacters :" configuration item.
3. Observe if there is a value following the colon and that the value is set to 1 as shown below:
   ```
   MinDevicePasswordComplexCharacters : 1
   ```
4. Search the outputted policy setting list for the "AlphanumericDevicePasswordRequired :" configuration item
5. Observe if the value following the colon is "True" as shown below:
   ```
   AlphanumericDevicePasswordRequired : True
   ```
6. Exit the Exchange Management Shell.

Remediation:

Using the Exchange Management Console (EMC):

In the "Properties" configuration window,

1. Click on the `Password` tab.
2. The "Require alphanumeric passcode" checkbox should be checked. When this checkbox is checked, you may enter the "Minimum number of complex characters" in the box on the right hand side.
3. Enter the number 1 in the box on the right hand side.
4. Click `OK`.

Using the Exchange Management Shell:

At the Exchange Management Shell command prompt,

1. Enter the following command (all one line):

```
Set-ActiveSyncMailboxPolicy -Identity "<PolicyName>"
 -AlphanumericDevicePasswordRequired $true
 -MinDevicePasswordComplexCharacters 1
```

   where <*PolicyName*> is the name of the Exchange ActiveSync mailbox policy for which the configuration should be made (replace brackets and text with appropriate policy name).

References:

1. NIST SP800-63-1, Electronic Authentication Guideline - Revision 1. Available: http://csrc.nist.gov/publications/nistpubs/800-63-1/SP-800-63-1.pdf

3.1.5 Set auto-lock timeout (Scored)

Profile Applicability:

- Level 1 - Apple iOS 5
- Level 2 - Apple iOS 5

Description:

The device can be configured to auto-lock after a pre-defined inactivity period. By default, if a passcode is defined, an iOS device will automatically lock after two minutes of inactivity, and the default Exchange ActiveSync policy setting applied for users not assigned to a mailbox policy sets an inactivity lock at 15 minutes. It is recommended that an inactivity timeout of no more than five (5) minutes be set for typical use cases and no more than two (2) minutes for high-security use cases.

Rationale:

Preventing the user from setting a long inactivity period reduces the risk that the iPhone will be unlocked in the event of a physical security breach.

Audit:

Using the Exchange Management Console (EMC):

In the "Properties" configuration window,

1. Click on the `Password` tab.
2. Observe if the "Time without user input before password must be re-entered (in minutes)" checkbox is selected.
3. Observe if the auto-lock timeout value is set to 5 or 2 according to use case.
4. Click `Cancel`.

Using the Exchange Management Shell:

At the Exchange Management Shell command prompt,

1. Enter the following command (all one line):

```
Get-ActiveSyncMailboxPolicy -Identity "<PolicyName>"
```

   where *<PolicyName>* is the name of the Exchange ActiveSync mailbox policy for which the audit validation should be made (replace brackets and text with appropriate policy name).

2. Search the outputted policy setting list for the "MaxInactivityTimeDeviceLock :" configuration item.
3. Observe if there is a value following the colon and that the value is set to 5 or 2 according to use case as shown below:

```
MaxInactivityTimeDeviceLock : 5
```

4. Exit the Exchange Management Shell.

Remediation:

Using the Exchange Management Console (EMC):

In the "Properties" configuration window,

1. Click on the `Password` tab.
2. Click on the "Time without user input before password must be re-entered (in minutes)" checkbox. When this checkbox is checked, you may enter the time in minutes for the auto-lock timeout in the box on the right hand side.
3. Set the Auto-lock interval:
   a) For typical use cases, enter the number 5 in the box on the right hand side.
   b) For high-security use cases, enter the number 2 in the box on the right hand side.
4. Click `OK`.

Using the Exchange Management Shell:

At the Exchange Management Shell command prompt,

1. Enter the following command (all one line):

```
Set-ActiveSyncMailboxPolicy -Identity "<PolicyName>"
 -MaxInactivityTimeDeviceLock: 00:05:00
```

where *<PolicyName>* is the name of the Exchange ActiveSync mailbox policy for which the configuration should be made (replace brackets and text with appropriate policy name) and specifying the time in minutes as appropriate according to use case and device as described for the EMC above.

3.1.6 Erase data upon excessive passcode failures (Scored)

Profile Applicability:

- Level 1 - Apple iOS 5
- Level 2 - Apple iOS 5

Description:

The device can be configured to erase the user's settings and data as stored on the device after excessive (configurable from 4 to 16) passcode failures. By default, the default Exchange ActiveSync policy setting applied for users not assigned to a mailbox policy configures the device to erase data after four (4) failed password attempts, if a password is configured on the device. It is recommended that this feature be enabled at six (6) failed password attempts.

Rationale:

Excessive password failures typically indicate that the device is out of physical control of its owner. Upon such an event, erasing data on the phone will ensure the confidentiality of information stored on the device is protected when facing a novice attacker.

Audit:

Using the Exchange Management Console (EMC):

In the "Properties" configuration window,

1. Click on the `Password` tab.
2. Observe if the "Number of failed attempts allowed:" checkbox is selected.
3. Observe if the failed attempts value is set to 6.
4. Click `Cancel`.

Using the Exchange Management Shell:

At the Exchange Management Shell command prompt,

1. Enter the following command (all one line):

```
Get-ActiveSyncMailboxPolicy -Identity "<PolicyName>"
```

   where <*PolicyName*> is the name of the Exchange ActiveSync mailbox policy for which the audit validation should be made (replace brackets and text with appropriate policy name).

2. Search the outputted policy setting list for the "MaxDevicePasswordFailedAttempts" configuration item.
3. Observe if there is a value following the colon and that the value is set to 6 as shown below:

   ```
   MaxDevicePasswordFailedAttempts : 6
   ```

4. Exit the Exchange Management Shell.

Remediation:

Using the Exchange Management Console (EMC):

In the "Properties" configuration window,

1. Click on the `Password` tab.
2. Click on the "Number of failed attempts allowed:" checkbox. When this checkbox is checked, you may enter the maximum number of failed attempts in the box on the right hand side.
3. Enter the number 6 in the box on the right hand side.
4. Click `OK`.

Using the Exchange Management Shell:

At the Exchange Management Shell command prompt,

1. Enter the following command (all one line):

```
Set-ActiveSyncMailboxPolicy -Identity "<PolicyName>"
 -MaxDevicePasswordFailedAttempts : 6
```

   where <*PolicyName*> is the name of the Exchange ActiveSync mailbox policy for which the configuration should be made (replace brackets and text with appropriate policy name).

Appendix: Change History

Date	Version	Changes for this version
03-27-2009	1.0.0	Public Release
10-30-2009	1.1.0	- Page 8, "Loss of Physical Custody of an iPhone and CompensatingControls": Addeddiscussion - Section 1.1.6, Turn off Auto-Join for all Wi-Fi networks: Inserted new section - Section 1.2.3, Enable Fraud Warning (Level 1, Not Scorable): Addednewsection - S
10-19-2010	1.2.0	Updated to cover iOS 4.1.0
06-10-2011	1.3.0	Expanded coverage for iPad, iPod and iPhone as well as cover iOS 4.3.0
12-31-2011	1.4.0	Updated to cover iOS 5