APPLE iOS
VERSION 5.1

Product Description

The Apple iOS is Apple's mobile operating system, running on a variety of devices including the iPhone and iPad. It contains a suite of hardware dependent applications including email, phone, enterprise applications, Internet and organiser information. The Apple iOS integrates with multiple Mobile Device Management servers which provide centralised management and control of iOS devices. The Apple iOS provides advanced security features to meet confidentiality and security requirements.

Evaluation Scope

The scope of the DSD Cryptographic Evaluation included the following functionality:

- Data protection
- Application sandboxing
- Remote management of the device

DSD's Findings and Recommendations

DSD performed a cryptographic evaluation on the product.

As iOS 5.1 has been evaluated with a DSD Cryptographic Evaluation, it can be used to downgrade the requirements for data at rest when data protection is used in combination with supervised mode.

DSD was able to confirm the implementation of encryption for data at rest. Data protection was found to securely encrypt the following stored user data:

- Mail – subject, email addresses, message body and attachments
- Mobile Safari

Refer to the iOS Hardening Guide for guidance on usage of 3rd party applications.

PROTECT

As such, the product can be used in accordance with the *Australian Government Information Security Manual* (ISM) for the storage of information of classifications:

- PROTECTED
- UNCLASSIFIED

Agencies should be aware that the reduction of storage and handling requirements for iOS 5.1 devices to those of UNCLASSIFIED is only in force when information is at rest. This applies only when devices are turned off or locked. Conversely, when a device is turned on and unlocked it takes the classification of the agency network to which it is connected. Agencies should develop Standard Operating Procedures (SOPs) for the protection of classified mobile devices to mitigate the threat of lost or stolen active devices.

As iOS 5.1 provides no security for voice calls, agencies MUST NOT use iOS 5.1 for classified phone calls. In addition, agencies MUST NOT use the SMS, MMS or iMessage capabilities of iOS 5.1 device to send any classified information.

For PROTECTED level networks, the chapter titled "Suggested Policies" in the *iOS Hardening Configuration Guide* is mandatory.

Additional Resources

Agencies wishing to use iOS 5.1 devices should refer to the ISM controls on Working Off-Site – Mobile Devices.

DSD provides a hardening guide for iOS 5.1. DSD recommends that agencies consider the implementation of as many recommendations as possible to increase the security of their deployed solution.

The *iOS Hardening Configuration Guide* is considered a compliance document for PROTECTED level networks ONLY (Chapter titled "Suggested Policies"), however it may assist agencies when connecting iOS devices to lower classified networks in complying with existing policies in the ISM.

The hardening guide is available from the DSD web site: www.dsd.gov.au.

Point of contact

For further information regarding certification, cryptographic evaluation or compliance with the ISM please contact DSD via email dsd.assist@defence.gov.au or 1300 CYBER1 (1300 292 371).