Description of document:	US Agency for International Development (USAID) iPad2 Risk Assessment, 2011
Requested date:	17-August-2011
Released date:	13-December-2011
Posted date:	26-December-2011
Title of document	Apple iPad2 Risk Assessment
Source of document:	FOIA REQUEST FOIA Team Leader Information & Records Division Office of Administrative Services United States Agency for International Development Room 2.07C, RRB Washington, D.C. 20523-2701 Fax: (202) 216-3070 Email: foia@usaid.gov

USAID
FROM THE AMERICAN PEOPLE

DEC 13 2011

RE: F-00251-11

This is in response to your August 17, 2011 request for a copy of "internal agency memos or other correspondence or documents that review or discuss the merits and/or disadvantages of iPads and similar pad/tablet computer devices for employee use", under the provision of the Freedom of Information Act [FOIA].

We are releasing 7 pages with limited redactions. Exemption 5 incorporates several civil discovery privileges, including the deliberative process privilege. The purpose of the privilege is to prevent injury to the quality of agency decisions by:

(1) Encouraging frank and open discussions on matters of policy between subordinates and superiors;
(2) Protecting against premature disclosure of proposed policies before final adoption;
(3) Protecting against public confusion that might result from disclosure of reasons and rationales that were not in fact ultimately the grounds for an agency's actions.

In this instance, the document proposes recommendations for policy changes and is not a final decision. Release of this deliberative process information to the public could hamper any final decision that might result from disclosure of reasons and rationales that were not in fact ultimately the grounds for our agency's actions.

Throughout the document you will see annotation of NR; these redactions are not responsive to your request.

You have the right to appeal these exemptions. Your appeal must be received in writing no later than 30 days from the date of this letter. In order for it to be considered **an official appeal,** it must be addressed as follows:

Director, Office of Management Services
U.S. Agency for International Development
Ronald Reagan Building, Room 2.12-010
Washington, DC 20523
202-216-3369 (fax)

Both the letter and the envelope must be plainly marked **"FOI APPEAL."** Please cite your FOIA tracking number [F-00251-11] in your letter.

There is no charge for processing this **FOIA** request.

Sincerely,

S. Lankford

S. Lankford
FOIA Team Leader
Information and Records Division
Office of Management Services

NR

Apple iPad2 Risk Assessment

Office of the Chief Information Security Officer

Version: 1.0
April 2011

NR

TABLE OF CONTENTS

USAID CISO Change Request Risk Assessment

1. PURPOSE

The purpose of this document is to provide a qualitative risk assessment of Change Requests (CRs) submitted to the CISO. The process determines the level of risk any given change will pose to the Confidentiality, Integrity, and Availability (CIA) Security Model of USAID Information Systems.

2. RISK ASSESSMENT APPROACH

This assessment is based on guidance adapted from NIST SP 800-53 Revision 3, *Recommended Security Controls for Federal Information Systems* and NIST SP 800-124, *Guidelines on Cell Phone and PDA Security*. The assessment is broad in scope and determines the level of risk the change request may potentially introduce to the USAID network. The Office of the CISO is not providing approval, rather submitting the possible risk to enable the Chief Information Security Officer to make an educated decision.

The Office of Security should be consulted to see if there are any concerns due to the new technology being used at USAID that may impact their respective offices, e.g. physical security.

3 RISK ASSESSMENT

The Office of the Chief Information Security Officer (CISO) has been tasked to perform a risk assessment for the **Apple iPad2**.

3.1 RISK IDENTIFICATION

The following is a list of identified technical risks which are present with an Apple iPad2. The i iPad2 uses an operating system (OS) originally designed for the iPhone and is called iPhone 4.3.2 OS.

Technical Related Risk

- **Unencrypted Data at Rest** – Not all data on the device is encrypted at rest, including but not limited to device location GPS history[1], logging of Wi-Fi access points encountered with corresponding GPS coordinates[2] and authentication credentials for common internet based applications[3]. The GPS tracking has been shown working even when the location services are

[1] Got an iPhone or 3G iPad? Apple is recording your moves. Retrieved April 21, 2011 - http://radar.oreilly.com/2011/04/apple-location-tracking.html

[2] Got an iPhone or 3G iPad? Apple is recording your move. Retrieved April 25, 2011 - http://radar.oreilly.com/2011/04/apple-location-tracking.html

[3] Will Mobile Apps be the Achilles' Heel of Web Security? http://research.zscaler.com/2011/04/will-mobile-apps-be-achilles-heel-of.html

NR

disabled[4]. These sensitive files are also stored unencrypted, by default, on any computer the device is synced with.

- **Privacy of Apps** – Applications available from the iTunes store regularly fail to fully disclose the device or personal data collected and to whom the data is being shared with. Furthermore the device does not make such communication available to the user for review[5]. This lack of disclosure to the handling of personal data on the device has led to an official inquiry from Congress[6].

- **Managing Applications** – As long as the iPad2 is not "jailbroken" or "hacked" the only place to get applications is the Apple Store. Although the Apple Store does its best to validate the code in applications sold on its online store, insecure applications will still be available and may add significant risk to USAID. In addition, applications that are not internally vetted through a Software Application Review may conflict with or adversely affect business operations or handling of Agency PII/SBU data.

- **Bluetooth Risk-** The iPad2 has an onboard Bluetooth radio and can pair with many different types of hardware. Bluetooth is an open standard for short-range radio frequency (RF) communication. Bluetooth technology is susceptible to the most common wireless networking threats, such as denial of service attacks, eavesdropping, man-in-the-middle attacks, message modification, and resource misappropriation. iPad2 Bluetooth configuration option through policy is limited to either allowing it or not and lack ability to restrict to specific Bluetooth profile. Most Bluetooth devices are promiscuous by default, responding to pages, service discovery probes, and connect requests.[7]

- **Wireless 802.11 Risk** – The iPad2 has an 802.11 radio installed enabling the iPad2 to wirelessly connect with compatible networks or be used as a wireless hotspot or access point. Wireless networking enables devices with wireless capabilities to use computing resources without being physically connected to a network. With 802.11 technologies, the major security threats are denial of service, eavesdropping, man-in-the-middle, masquerading, message modification, message replay, and traffic analysis.[8]

[4] IPhone Stored Location in Test Even if Disabled. Retrieved April 25, 2011 http://online.wsj.com/article/SB10001424052748704123204576283580249161342.html#ixzz1KaTRoFzc

[5] Your Apps Are Watching You retrieved April 21, 2011 http://online.wsj.com/article/SB10001424052748704694004576020083703574602.html

[6] Apple faces questions from Congress about iPhone tracking. Retrieved April 24, 2011 http://www.computerworld.com/s/article/9216058/Apple_faces_questions_from_Congress_about_iPhone_tracking

[7] National Institute of Standards and Technology. Guide to Bluetooth Security. Retrieved June 04, 2010, *http://csrc.nist.gov/publications/nistpubs/800-121/SP800-121.pdf*

[8] National Institute of Standards and Technology. Establishing Wireless Robust Security Networks. Retrieved June 04, 2010. http://csrc.nist.gov/publications/nistpubs/800-97/SP800-97.pdf

NR

- **Vulnerability Exploitation** – New vulnerabilities discovered in the Bluetooth stack, or in the iPad2 software, may result in new exploits that current controls cannot mitigate providing additional threat vectors for compromise.[9]

- **iPad2 Accessories -** The iPad2 can connect with many types of accessories, most notably Bluetooth Keyboards and USB devices. Currently, there are no Bluetooth keyboards that support FIPS 140-2 that are compatible with the iPad2.

Business Related Risk

(b)(5)

3.2 RISK DETERMINATION

Based on our assessment, we determined that the functionality poses a Risk and requires the appropriate risk-reducing controls to decrease the risk to an acceptable level.

3.3 CONTROL RECOMMENDATIONS

The goal of the recommended controls is to reduce the level of risk to the USAID network and its data to an acceptable level. The following are recommended controls that could mitigate or eliminate the identified risks, as appropriate to USAID operations. However, the controls recommended **do not guarantee** a secure Apple iPad2deployment and cannot prevent all threats.

Standard Configuration - Research, identify, test, document and implement standard configuration for USAID issued iPads to include but not limited to the iPhone OS and supported applications authorized by USAID.

[9] National Institute of Standards and Technology. Guide to Bluetooth Security. Retrieved June 04, 2010, *http://csrc.nist.gov/publications/nistpubs/800-121/SP800-121.pdf*

NR

Unencrypted Data at Rest – It is recommend that Agency data stored on device should be kept within or access through an application that has NIST validated 140-2 encryption of data at rest and encryption of data during communication to agency services.

Privacy of Apps – Applications chosen for processing or storing Agency information should follow Software Application Review process to ascertain risk exposure to PII/SBU.

(b)(5)

iPad2 Accessories - USAID and other federal agencies must use Federal Information Processing Standard (FIPS) 140-2, *Security Requirements for Cryptographic Modules*, when it is determined that information must be protected by cryptography. To protect sensitive information, we recommend employ a FIPS 140-2 cryptographic module. Wireless keyboards currently available on the market as accessories for the iPad do not support FIPS 140-2, or AES-256. However, wireless keyboards presently support AES-128.

(b)(5)

Additional Reference – Please reference NIST SP 800-124, *Guidelines on Cell Phone and PDA Security* for additional guidance. Please also referent Apple's technical documentation relating to enterprise deployment/configuration and securing devices that run their iOS software: iPhone OS Enterprise Deployment Guide; iPhone in Business Security Overview; and iOS Configuration Profile Utility.[12]

Document Control

NR

[10] http://developer.apple.com/library/ios/#documentation/NetworkingInternet/Conceptual/iPhoneOTAConfiguration/Introduction/Introduction.html#//apple_ref/doc/uid/TP40009505

[11] http://images.apple.com/ipad/business/pdf/iPad_Security_Overview.pdf

[12] http://developer.apple.com/library/ios/navigation/index.html#filter=Enterprise%20Deployment

NR

NR

USAID CISO Change Request Risk Assessment

NR

NR