



# governmentattic.org

*"Rummaging in the government's attic"*

Description of document: Bureau of Land Management (BLM)  
memos/correspondence/documents reviewing/discussing  
the merits and/or disadvantages of iPads and/or similar  
pad/tablet computer devices for employee use, 2010-2011

Requested date: 15-August-2011

Released date: 04-October-2011

Posted date: 14-November-2011

Source of document: Headquarters, Washington Office Bureau of Land  
Management  
FOIA Coordinator  
M. Street, 3rd floor, WO 560  
1849 C. St. NW  
Washington, D.C. 20240  
Fax: 202-245-0027  
Email: [BLM\\_WO\\_FOIA@BLM.GOV](mailto:BLM_WO_FOIA@BLM.GOV)

## Note:

The governmentattic.org web site ("the site") is noncommercial and free to the public. The site and materials made available on the site, such as this file, are for reference only. The governmentattic.org web site and its principals have made every effort to make this information as complete and as accurate as possible, however, there may be mistakes and omissions, both typographical and in content. The governmentattic.org web site and its principals shall have neither liability nor responsibility to any person or entity with respect to any loss or damage caused, or alleged to have been caused, directly or indirectly, by the information provided on the governmentattic.org web site or in this file. The public records published on the site were obtained from government agencies using proper legal channels. Each document is identified as to the source. Any concerns about the contents of the site should be directed to the agency originating the document in question. GovernmentAttic.org is not responsible for the contents of documents published on the website.



United States Department of the Interior  
BUREAU OF LAND MANAGEMENT  
Washington, D.C. 20240-0036  
<http://www.blm.gov>



October 04, 2011

In Reply Refer To:  
1278-FOIA (560)  
FOIA No. 2011-01067


This letter is in response to your Freedom of Information Act (FOIA) request, dated August 15, 2011, for information relating to:

“...internal agency (BLM) memos or other correspondence or documents that review or discuss the merits and/or disadvantages of iPads and/or similar pad/tablet computer devices for employee use.”

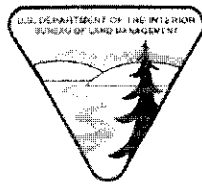
In accordance with our letter dated, September 09, 2011, we have enclosed approximately 79 pages of responsive records in their entirety.

Thank you for your interest in our public lands and in the programs and activities of the BLM. If you have any questions regarding request, please contact Jayson D. Ellwein, BLM WO FOIA Specialist at (202) 912-7564 or by Email at [jdellwei@blm.gov](mailto:jdellwei@blm.gov).

Sincerely,

  
Paulette L. Sanford  
Chief, Division of IRM Governance

Enclosures



**UNITED STATES DEPARTMENT OF THE INTERIOR  
BUREAU OF LAND MANAGEMENT  
WASHINGTON, D.C. 20240**

**To:** Idaho State Office, Alaska State Office, Cadastral Program, and Network Operations Center (NOC)

**From:** Division Chief, Business and Technology Alignment Division (WO-570)

**Subject:** Tabular PC Pilot

The BLM Information Resources Management (WO-500), Business and Technology Alignment Division (WO-570) are pleased to announce the launch the Tabular PC Pilot, as a part of the mobile workforce initiative to encourage “anywhere, anytime” BLM availability. The pilot will take place for 120 days in three concurrent phases, technology, End User testing, and cadastral surveying. The technology phase will examine the network operations, security, and enterprise architecture associated with adding tabular PCs to the BLM infrastructure. End Users will evaluate the tabular devices as a day to day operational device to conduct BLM business. The Cadastral Surveying phase will provide evaluation of the tabular devices in real-time field operations.

A Tabular Pilot site has been created (<http://teamspace/sites-wo/wo500/Pilot>) so participants in the pilot can share experiences, log questions, receive instructions, and monitor the overall pilot project.

Below is a list of the participants in the Tabular PC Pilot Project.

- **Technology**
  - *Enterprise Architecture (WO-570)*
  - *Security (WO-590)*
  - *Network Operations (NOC)*
- **End User Testing**
  - *Information Technology Investment Board (ITIB)*
    - *Washington Office, Idaho State Office, and Alaska State Office*
- **Cadastral Surveyors**
  - *Washington Office and State Representatives*

Please direct all questions regarding this pilot to Kerry Lewis (WO-570) at 202-912-7581, [kerry\\_lewis@blm.gov](mailto:kerry_lewis@blm.gov).



**UNITED STATES DEPARTMENT OF THE INTERIOR  
BUREAU OF LAND MANAGEMENT  
WASHINGTON, D.C. 20240**

**To:** Washington Office, Idaho State Office, Alaska State Office, Cadastral Program,  
and Network Operations Center (NOC)

**From:** Division Chief, Business and Technology Alignment Division (WO-570)

**Subject:** Tabular PC Pilot

The BLM Information Resources Management (WO-500), Business and Technology Alignment Division (WO-570) are pleased to announce an extension of the Tabular PC Pilot period. The pilot will take place for an additional 90 days to incorporate email capability, cadastral surveying phase of the pilot, and a very limited number of alternative tabular PC devices.

A Tabular Pilot SharePoint site has been created (<http://teamspace/sites/wo-wo500/Pilot>) so participants in the pilot can complete and submit device evaluation criteria requirements. On the SharePoint site you will find mandatory pilot surveys and questionnaires related to implementation, configuration, applications, and mandatory file downloads and white papers associated with pilot devices. Current pilot participants are required to comply with all documents/requirements currently listed in the Phase I folder of the site as soon as possible.

The technology phase was assigned the examination of network operations, security, and enterprise architecture associated with adding tabular PCs to the BLM infrastructure. Please submit your finding, lessons learned, and configuration white papers to WO-570 by September 30, 2011.

Please direct all questions regarding this pilot to Kerry Lewis (WO-570) at 202-912-7581, [kerry\\_lewis@blm.gov](mailto:kerry_lewis@blm.gov).

**Challenge:** The Bureau spends about \$1300 (check ITILoB) to purchase computers for its employees. It spends an average of \$1300/yr for five years supporting these machines. An iPad costs approximately \$500.00 and is based on an embedded operating system that requires very little maintenance, so this device has the potential to save thousands of dollars over its lifespan.

The challenge is whether the iPad could be used as a form of a thin client terminal and serve as a viable replacement for many of these workstations.

The iPad has several secondary considerations that could result in additional costs savings:

1. These devices include cellphone capability, so it may be possible to reduce infrastructure costs in the offices by reducing the need to install a wired network.
2. These devices include their own monitor, so the cost of a monitor is avoided. They have a USB interface, so it may be possible to support a second monitor if that monitor had a USB Interface.
3. It is possible to take these devices to the field and to meetings, so they may provide ubiquitous access to data, potentially reducing the dependency on such devices as thumb drives.
4. These devices include GPS capability, which would provide a valuable navigation tool for the Bureau's mobile workforce.
5. These devices could potentially further reduce the necessity for IT support staff by using Apple's mail back maintenance plan.
6. These devices can use cell based technology, potentially reducing cost for the organization by replacing the desktop phone.

**Context of the initiative:** The Bureau of Land Management has 10,000 to 16,000 employees. On average, there are 1.6 computers per employee. Computers cost the bureau around \$1300.00 each and are on a 5 year refresh schedule. Given these figures, the Bureau has between \$20,800,000 and \$33,290,000 tied up in desktop hardware. Approximately 1/5 of this is replaced each year at a cost of between \$4M and \$7M.

If iPads could be used as substitute devices on the desktop, the bureau could reduce its capital investment in half for this class of devices to between \$8M and 12M.

Since iPads are mobile devices, it is likely that further savings will be realized because the ratio of 1.6 computers per person could be reduced because employees will no longer need to have a second computer to travel with. The same machine could be used on the desktop and as a mobile device. While this will not completely eliminate such duplication, it is reasonable to expect the ratio to lower to something on the order of 1.2 devices per person (a savings of as many as 6,400 devices).

Given that iPads are upgradeable remotely and the embedded nature of their software it is entirely possible that their refresh cycle could be longer than PCs. It is reasonable to estimate somewhere in the neighborhood of seven years, thus further reducing overall costs.

One of the other significant opportunities for savings is in support and maintenance. Given that the operating system is embedded and the entire device can be refreshed remotely, it is entirely likely that the support costs could be dramatically reduced. Not enough empirical data is available at this time to provide an estimate about how much less.

Using an iPad instead of a laptop with a BlackBerry/AirCard, or cellphone modem could save money by avoiding the necessity of purchasing and managing these devices. Currently, there is a requirement to use AT&T as the provider. This needs to be evaluated on its own merit.

**Risks:** The iPad is not without risk. There are three major areas of concern:

1. Software Incompatibility – The iPad does not support .pdfs or flash. How important these are remains to be seen.
2. Not all software is web based – Some experimentation would be needed to find out how much could be done with the built in word processing software versus web based software or Citrix based software.
3. The security setup would need to be figured out.

**Actions required:**

The device has many potential advantages, but along with this there is significant risk. The risks associated with web based software apply across the board. This issue needs to be addressed regardless of which desktop or mobile platform is chosen.

Because of the potential for savings and because so many things are unknown about these devices (and other mobile thin clients), it is recommended that several of these units be purchased and evaluated.

**Results:**

**Anticipated Results:** The results anticipated from this effort are:

1. > 30% reduction in capital expenditure for desktop computing
2. > 30% reduction in trouble tickets pertaining to desktop support
3. Reduction of computers per person from a ratio of 1.6:1 to 1.2:1
4. Reduction in the number of remote access modems such as AirCards
5. Issues about thin client functionality will be fleshed out
6. Security concerns related to thin clients will be resolved.

**Actual Results:** TBD

**Lead:** Patrick Stingley

**Status**

July 26<sup>th</sup> – This item was not discussed, but per Ronnie's request during the meeting an attempt was made to purchase iPads for each of the participants. In addition, a protective cover, a stand so they could be used on a desk, a USB-to-Ethernet adapter so they could connect to the wired network, a keyboard/mouse combination and a USB hub were specified. The Purchase Order has not been approved

From a business perspective, the Tablet PC that runs Windows XP Tablet PC Edition is expected to transform the way IT pros work by providing a completely new method for inputting information. This proclamation from our technology sector sounds like a pretty big boast, especially from an industry that was built by working solely with a keyboard and mouse.

While the idea of pen-based computing is not entirely new, making it work in a business environment is. There are bound to be opportunities that will develop because of the Tablet PC, but the real issue is deciding whether it is time to invest in this technology now or whether it is better to wait for the next version. So, if you are on the cusp of making a hardware upgrade soon, it helps to understand your needs before investing in this new technology. Making a business case for the Tablet PC really depends on a few factors, which I'll go over in this article.

#### Disclaimer

I currently use a Tablet PC at work. Mine is a terrific [ViewSonic V1100](#) that I started using as a demo model before eventually using it as one of my day-to-day computers for tasks here at the office.

#### The ultimate note taker

Do your users attend a lot of meetings? If so, the feature that strikes most people as revolutionary about the Tablet PC is the note-taking capabilities of Microsoft Journal. It's the most natural note-taking technology to date. Working with Microsoft Journal eliminates the need for pen and paper at meetings. A user can begin using this application with minimal computer experience. Also, having a centralized note-taking device will eliminate the double entry that usually takes place after a meeting once a user has returned to the office.

#### Laptop replacement

If your sales force carries laptops, the Tablet PC is a natural fit for these users. Essentially, the Tablet PC with Windows XP Tablet PC Edition is a super laptop with a fully functioning Windows XP operating system. When choosing between a laptop and the Tablet PC, the Tablet PC is preferable because, in terms of features, it is identical to its laptop cousins and includes additional features, such as the aforementioned Microsoft Journal.

#### Better workflow

The Tablet PC changes workflow problems encountered with traditional desktop and laptop systems because it allows source documents to reside within the unit. When source documents are paper based, the next logical step in the entry process is reentry, which is not a productive use of time. Now users can pull up predeveloped forms on a Tablet PC that include drop-down lists and dialog boxes to ease data entry. For instance, an insurance claims adjuster can examine a vehicle involved in an accident and fill out a claim form on the Tablet PC. The adjuster can make notations about the accident in predefined areas of the form and fill in the information required to complete the form. From there the form can be wirelessly transmitted to its next destination.



### Small transition issues

Your users should already be familiar with PC operating systems. The Tablet PC with Windows XP Tablet PC Edition does not require a great deal of transition time since it's based on an already established platform. Also, if a user prefers typing and using a mouse for input, then the units are equipped to handle those methods as well. However, most users will take to the natural feel of digital ink since it's identical to writing on a piece of paper.

What will take time is getting users to realize the opportunities to use the Tablet PC as a collaborative device. Taking notes and jotting down ideas is one thing; sharing them wirelessly within a group may go overlooked. There are many features embedded within the Tablet PC that make sharing possible, but users might take a while to adjust to this new way of communicating.

### Niche use

Tablet PCs have been referred to as niche industry devices. One of the first industries to beta test Tablet PCs was the healthcare industry. Small pockets of healthcare professionals, from doctors to administrative staff, became Tablet PC-enabled to determine whether these devices would enhance their work lives. The benefits proved dramatic as they enabled a paper-intensive industry to streamline its workflow digitally.

As an IT manager, you will ultimately have to decide whether the industry your company competes in is positioned to take advantage of this new way of working. If the bottlenecks in your workflow are paper intensive, then the Tablet PC could help to eliminate them.

### Instant-on capability

The instant-on feature found in today's handheld PDAs is a feature sorely lacking in Tablet PCs. Stopping to wait for a boot process when all you want to do is jot a few notes down is not a good use of your time. However, if you are looking to replace laptops in your organization, then this inconvenience is minimized by the fact that laptops are not instant-on-enabled either.

### Development is playing catch up

While much can be said for the Tablet PC's unique way of inputting information, there is still a dearth of business applications that harness the true power of digital ink technology for the devices. Currently, the development community is struggling with the new coding idiosyncrasies that make the Tablet PC work, so if users are in a hurry to see all their forms on one machine, they may be disappointed. However, I'm confident this void will be filled, as many software companies have devoted their resources to Tablet PC application development.

### Cost factor

The last issue is the cost factor. Like all new technologies, Tablet PCs are priced in the high

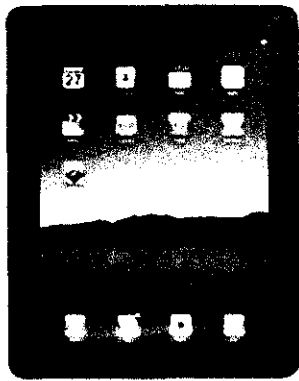
range when compared to a traditional laptop. Depending on the model and type (slate vs. convertible), the average price range for a new Tablet PC starts at around \$1,800. They are equipped with all the features of modern laptop, but at that price point you can typically purchase two high-end laptops for the price of one Tablet PC. Over time you can expect these prices to fall, but if you do wait, you will miss out on the many features that are already built into the Tablet PC that could provide immediate benefits to your users.

## Tablet PCs – There's an app for that

Tablet PCs and more notably the iPad ([www.ipad.com](http://www.ipad.com)) are all the rage – not only can I comfortably read my the headlines from all of my favorite news outlets through a single view via Pulse, ([www.alphamobilelabs.com](http://www.alphamobilelabs.com)) while listening to my free Internet radio channel ([www.pandora.com](http://www.pandora.com)) and wrestling my iPad from my kids to play our favorite game, Angry Birds (<http://tinyurl.com/y7soibh>), I can even use it to lock the doors on my house and turn down the A/C (<http://bit.ly/eAaH5>) while sitting in the airport. As cool as these new gadgets are, can they help us more efficiently accomplish BLM's mission?

### There's an App for That

Don Buhler, Chief for Cadastral Survey within the Division of Lands, Realty and Cadastral Survey, certainly thinks so. His team of surveyors usually carries loads of printed documents (maps, plats, etc.)



into the field to survey boundaries of our public lands. Through a pilot conducted in coordination with IRM, Don's team will now carry tablet PCs into the field. Browse to the [GLO Records](http://www.glorecords.blm.gov) web site to download original surveys, plats and field notes; access [Google Earth](http://www.google.com/earth) to overlay a visual image of the current terrain on an original map; strike up [GPS](http://www.google.com/gps) to validate longitude and latitude coordinates and now we're cooking with oil. "Defining our land's boundaries was never so easy," says Don Buhler, "We expect to significantly cut our time to survey by leveraging the latest applications such as GPS and the mobility of tablet PCs." Pretty cool, huh?

### Tablet PCs vs. Laptops

If you're like me, you might be wondering whether we can do all these cool things on our existing laptops or even PDAs/cell phones. The answer is largely, "yes", you can do many of these things on a PC, but are you going to be carrying your laptop around like you do your cell phone? And while your cell phone/PDA is mobile enough to take it anywhere with you, it's far from optimal if not impossible to use GLO (BLM's General Land Office [www.glorecords.blm.gov](http://www.glorecords.blm.gov)) and many other applications from your cell phone/pda (unless you've got a magnifying glass and really small fingers :-). The fact is that at roughly 8-10 inches high x 6-7 inches wide x ½ an inch thick and 1.5 pounds, tablet PCs hit that sweet spot of mobility, legibility and manipulability that laptops and PDA/phones just haven't been able to accomplish, making them ideal for highly mobile professionals and in particular, those who are operate in the field.

#### iPad

[HP Pavilion tx2500z](#)

[Samsung Galaxy Tab](#)

[Lenovo ThinkPad X61 Tablet PC](#)

[Dell Inspiron Duo](#)

In addition to email, web browsing and word processing, tablet PCs provide unique functionality, not available via the standard laptop PC. One such capability, often referred to as “digital ink”, enables you to use your natural writing device, a pen as digital ink, to capture thoughts, draw and annotate and when coupled with the tablet PCs flat working surface provides a powerful tool, as well as a simple method for obtaining signatures on documents.

Laptops, however, provide for faster input via traditional keyboards, bigger monitors and are better when it comes to printing and sharing files. In the final analysis, tablet PCs and laptops offer very similar functionality each with their own advantages (see the table below) with the primary difference being the ultra-portability offered by the tablet PC.

Tablet PCs	Laptops
Lighter and more mobile	Better print capability
Flat working surface	Easier to save/share files
Personalized input (digital ink using a finger or pen)	Bigger monitors
Longer battery life	Easier to use keyboards, faster input
Lower heat and power draw processors	Built in optical (DVD) drives
Lower overall cost	Can run desktop applications (vs. web apps)

### **All That and Lower Cost Too?**

But what about the cost of these new gadgets? According to an IRM study into the feasibility of tablet PCs for use at BLM, at a roughly \$600 purchase price (vs. the current BLM cost of \$1,300 per employee for a laptop) and with its embedded, low-cost to maintain operating system, these new devices make a strong case for cost reduction over traditional laptops. Further, if tablet PCs can be used as a thin client terminal along with a docking station, it has the potential to replace many of BLM’s workstations altogether and help to significantly reduce BLM’s current ratio of 1.6 computers per employee.

### **OK, What’s the Downside?**

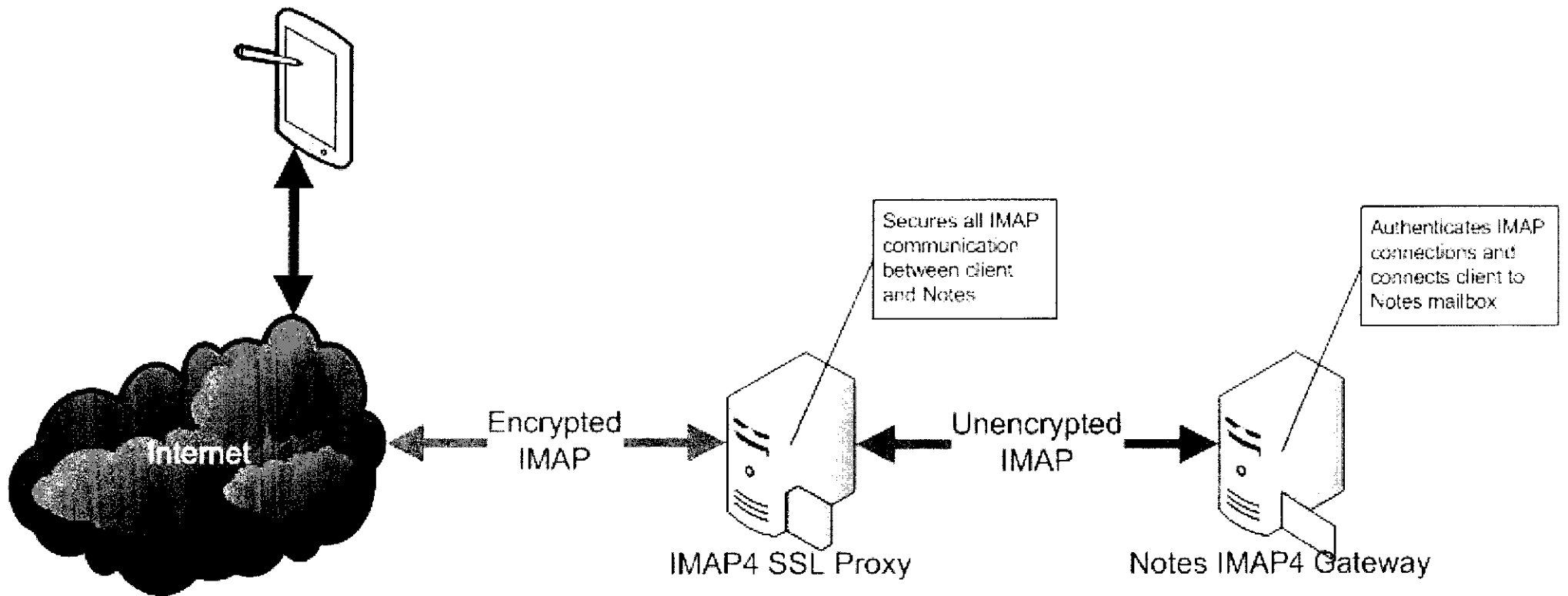
While there are manageable issues such as security and printing to be worked out, the primary concern for the Bureau to resolve before we can see widespread use of tablet PCs is software compatibility and availability. Certain applications like Flash and PDFs are not effectively supported by tablet PCs and some of BLM’s applications are not web applications nor designed to be run on tablet PCs.

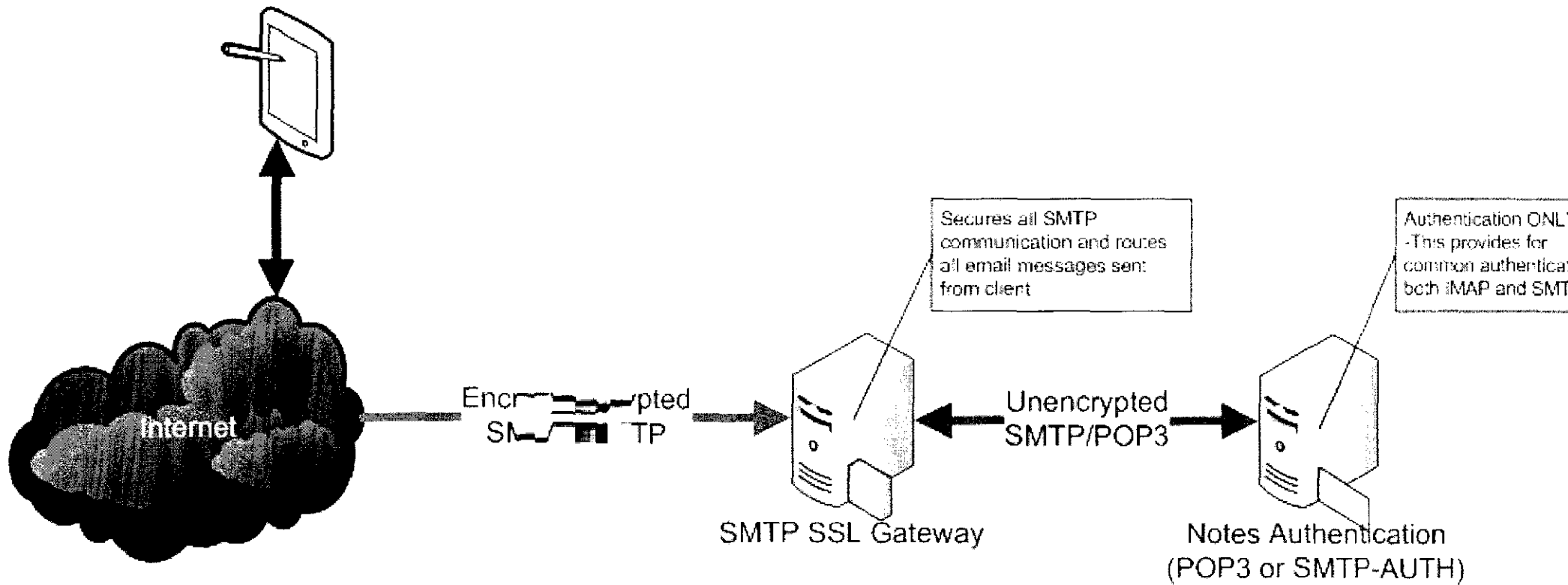
### **So When Can I Get My Tablet PC?**

Leading the tablet PC charge for BLM is IRM’s Division of Business and Technology Alignment, which is currently conducting a 120 day pilot with Cadastral Survey within the Division of Lands, Realty and Cadastral Survey. The Cadastral Survey Group will receive a tablet PC for each of its State representatives and Washington, DC office staff to test their applicability in the field. Additionally, IRM is conducting a pilot with members of the IT Investment Board (ITIB). “Through the pilot, IRM will determine an optimal image of tablet PC applications for the Bureau, as well as sort out access, security and procurement procedures,” explains Al’Tariq Samuels, IRM’s Division Chief for Business and

Technology Alignment. “With the implementation of tablet PCs BLM employees will have real-time, highly mobile access to the BLM network and the information needed to accomplish our mission,” says Al’Tariq. In the meantime, if you have an idea of how tablet PCs can help BLM better accomplish its mission, click [HERE](#) [links to a form that emails feedback to [BLM\\_IRMcNewsletter@blm.gov](mailto:BLM_IRMcNewsletter@blm.gov) and has the following subject line: eNewsletter Tablet PCs] to let us know!

**Contributing Authors:** Al’Tariq Samuels and Kerry Lewis





## Summary

BLM – Alaska acquired permission from WO500 and the BLM National Operations Center to acquire and deploy one (1) Apple iPad and one (1) Research in Motion (RIM) Playbook in the Alaska portion of the BLM General Support System (GSS). This whitepaper is intended to describe the lessons learned to-date on this deployment. These systems have been assigned to the Alaska State Director (the iPad) and a systems administrator (the RIM Blackberry) who also supports the iPad.

### BLM – Alaska's request

BLM – Alaska requested to be part of the BLM test bed of tablet devices. Initially an Apple iPad was assigned to the Alaska State Director (SD). In July Alaska also requested to acquire a Research in Motion (RIM) Playbook. We were interested in testing the Playbook because the Blackberry systems are the approved portable devices. BLM- Alaska has approximately 90 Blackberry users in the state.

### BLM – Alaska's Approach

The iPad assigned to the SD has been deployed with this functionality:

- Virtual Private Networking (VPN) into the DOI/BLM network
- BLM electronic mail access through Lotus Notes imap protocols
- An MS Word compatible document processing application
- An MS Power Point compatible overhead processing application
- An MS Excel compatible spreadsheet processing application
- A web browsing application
- CITRIX access for network applications and data

The RIM Playbook was connected to a RIM Blackberry cell phone (Storm) using the RIM "bridge" functionality. Applications on the Playbook included:

- BLM electronic mail access through Lotus Notes the Blackberry Enterprise Service (BES)
- An MS Word compatible document processing application
- An MS Power Point compatible overhead processing application
- An MS Excel compatible spreadsheet processing application
- A web browsing application

### What we've found so far

#### iPAD

The iPad assigned to Alaska is used daily by the State Director. The SD has found it invaluable as a work tool. He is able to send and receive BLM email and open attachments. Initial connectivity issues were resolved and the system has been working fairly well since being deployed.



The SD was recently able to use the iPad in a remote field camp (Bering Glacier) via a WIFI in the camp.

Since the iPad utilizes an IMAP connection to email it does not support access to the corporate calendar or email contacts list.

### **RIM Playbook**

The RIM Playbook is used daily to retrieve email and email attachments. The system has a fairly fast response rate but is slow to initiate. Connecting the Blackberry and Playbook adds steps to starting the system, but is accommodated by software buttons on each piece of equipment.

The user has access to BLM email, contacts, and calendar information that is presented through the Blackberry Enterprise Server.

Through the RIM Bridge application and connectivity this tablet maintains the same encryption that is native to the Blackberry system. The user must enter the same passcode key for encryption on the Playbook that is used on the Blackberry phone. Once the connection is broken the email data on the tablet goes away.

The Playbook is a 7" diagonal tablet; the user has not experienced usability issues with the smaller device. Because this device is smaller the screen and images seem sharper than on the larger iPad tablet.

Since the Playbook is connected to the Blackberry Enterprise Server it has full access to corporate email, calendaring and contacts.

### **Mission Needs Met**

Up to this point the missions needs met by deploying these system have been:

- Light weight portability
- With the Playbook access to corporate email, calendaring, and contacts
- Access to the BLM networked applications and data through the VPN environment.

### **Next Steps**

From what we have seen so far; the Playbook extends the existing capabilities of the Blackberry phone.

BLM – AK would like to pursue this opportunity and acquire more Playbooks and get more users involved with testing, preferably non-IT staff; that would include a cross section of managers and heavy duty Blackberry users. We are requesting adding up to 10 playbooks to the test environment.

Beyond typical email/calendar functionality we would like to test more complex access through the Playbook platform; such as:

- ArcGIS
- CITRIX access to networked data and applications

### **Points of Contact for this project**

Garth Olson  
Chief, Branch of Information Resources  
Management  
Phone – 907.271.5545  
Email – [g2olson@blm.gov](mailto:g2olson@blm.gov)

Mark Withey  
Systems Administrator  
Phone – 907.271.3796  
Email – [mwithey@blm.gov](mailto:mwithey@blm.gov)



**DRAFT**

# **APPLE iOS 4 TECHNOLOGY OVERVIEW (for iPhone, iPad, and iPod Touch)**

Version 1, Release 0.1

21 September 2010

**Developed by DISA for the DoD**

**UNCLASSIFIED**

This page is intentionally left blank.

## TABLE OF CONTENTS

	<b>Page</b>
<b>1. INTRODUCTION.....</b>	<b>1</b>
1.1 Background.....	1
1.2 Authority.....	1
1.3 Scope.....	2
1.4 Vulnerability Severity Code Definitions .....	2
1.5 STIG Distribution .....	5
1.6 Document Revisions .....	5
<b>2. IPHONE AND IPAD DEVICE AND GOOD SERVER SECURITY INFORMATION 7</b>	
2.1 Application Repository and Deployment.....	7
2.2 Provisioning Procedures .....	8
2.3 Procedures For Changing Device Applications.....	9
2.4 PKI Support .....	10
2.4.1 S/MIME Configuration.....	10
2.4.2 Using Software Certificates .....	11
2.5 Remote Connections to DoD Networks.....	11
2.6 Disposal of iPhone and iPad Devices .....	11
2.7 Antivirus Support on iPhone and iPad Devices.....	11
2.8 iPhone Instant Messaging (IM).....	12
2.9 Enterprise Firewall Configuration .....	12
2.10 Wi-Fi Configuration.....	14
2.10.1 Wi-Fi Connection to a DoD-Operated Enterprise WLAN System.....	14
2.10.2 Wi-Fi Connection to a Public Hot Spot WLAN System .....	14
2.10.3 Wi-Fi Connection to a Home WLAN System .....	14
2.11 Bluetooth Configuration .....	14
2.12 Tethered Modem Use.....	14
<b>APPENDIX A. IOS DEVICE SYSTEM ADMINISTRATOR SECURITY CONFIGURATION TASKS.....</b>	<b>15</b>
<b>APPENDIX B. IPHONE AND IPAD DISPOSAL PROCEDURES .....</b>	<b>17</b>
<b>APPENDIX C. GOOD MOBILE CONTROL AND END USER S/MIME CONFIGURATION.....</b>	<b>19</b>
C.1 Run InstallRoot on Good Mobile Control (GMC) Server .....	19
C.2 Obtain SSL Certificate for GMC Server.....	19
C.3 Configure GMC Server to use DoD SSL Certificate.....	19
C.4 Server Configuration.....	20
C.5 Initial User Configuration .....	21
C.6 Setup Procedure When User Is Issued New Credentials (Or Loss of SCR).....	23
<b>APPENDIX D. VMS PROCEDURES.....</b>	<b>25</b>

## LIST OF TABLES

	Page
Table 1-1. Vulnerability Severity Category Code Definitions .....	2
Table 2-1. Apple Device Provisioning Procedures.....	8
Table 2-2. Apple Device Application Change Procedures .....	9
Table 2-3. Host-Based Firewall Architecture on GFE Server .....	13

## LIST OF FIGURES

	Page
Figure C-1. S/MIME Server Configuration .....	21
Figure C-2. Good Mobile Control Self Service Portal .....	22

## 1. INTRODUCTION

### 1.1 Background

The iPhone/iPad Security Technical Implementation Guide (STIG) and associated documents (e.g., Apple iOS 4 Technology Overview, Good Technology iOS Hardening Guide, Apple iOS 4 (with Good Mobility Suite) STIG, Good Mobility Suite Server (iOS) STIG, Smartphone Policy STIG, General Wireless Policy STIG and Wireless Management Server Policy STIG), provide security policy and configuration requirements for the use of any handheld device using Apple iOS 4 (such as iPhone, iPad, or iPod Touch) in the Department of Defense (DoD). Guidance in these documents applies to all DoD iPhone, iPad, and iPod Touch systems used to store, process, transmit, or receive DoD information. This STIG applies to iPhone models 3GS and 4 using Apple iOS 4.x (earlier models should not be used within the DoD), iPad devices using OS 3.2 or iOS 4.x and iPod Touch 3<sup>rd</sup> generation devices. Note: DoD iPads with OS 3.2 should be upgraded to iOS 4.x as soon as it is available.

The initial version of the STIG requires the use of Good Technology's Good Mobility Suite (GMS) to provide secure email, security policy management, and data protection services on DoD iPhone, iPad, and iPod Touch devices. Future versions of the iPhone/iPad STIG may include other third-party vendor security products or a "native" iOS configuration when it has been determined that they provide required DoD security controls.

The STIG serves as both a security review checklist and a configuration guide. Information Assurance Officers (IAOs), Security Managers (SMs), System Administrators (SAs), device users, and Security Readiness Review (SRR) Reviewers should use the STIG to ensure the security of DoD iOS 4 devices.

This STIG has the minimum "baseline" Apple iOS 4 security guidance for DoD. Combatant Commanders/Services/Agencies (CC/S/A) may direct more secure configuration settings based on operational requirements.

**Note: Unless specifically indicated otherwise, when the term "iPhone" is used in this document it will include iPhone, iPad, and iPod Touch devices.**

### 1.2 Authority

DoD Directive (DoDD) 8500.1 requires that "all IA and IA-enabled IT products incorporated into DoD information systems shall be configured in accordance with DoD-approved security configuration guidelines" and tasks Defense Information Systems Agency (DISA) to "develop and provide security configuration guidance for IA and IA-enabled IT products in coordination with Director, NSA." This document is provided under the authority of DoDD 8500.1.

Although the use of the principles and guidelines in this STIG provide an environment that contributes to the security requirements of DoD systems operating at Mission Assurance Categories (MACs) I through III, applicable DoD Instruction (DoDI) 8500.2 Information Assurance (IA) controls need to be applied to all systems and architectures.

The Information Operations Condition (INFOCON) for the DoD recommends actions during periods when a heightened defensive posture is required to protect DoD computer networks from attack. The IAO will ensure compliance with the security requirements of the current INFOCON level and will modify security requirements to comply with this guidance.

The Cyber Command (CYBERCOM) has also established requirements (i.e., timelines) for training, verification, installation, and progress reporting. These guidelines can be found on their web site: <https://www.cybercom.mil>.

Initially, these directives are discussed and released as Warning Orders (WARNORDs) and feedback to USCYBERCOM is encouraged. USCYBERCOM may then upgrade these orders to directives; they are then called Communication Tasking Orders (CTOs). It is each organization's responsibility to take action by complying with the CTOs and reporting compliance via their respective Computer Network Defense Service Provider (CNDSP).

### 1.3 Scope

This document is a requirement for all DoD-administered systems and all systems connected to DoD networks. These requirements are designed to assist SMs, Information Assurance Managers (IAMs), IAOs, and SAs with configuring and maintaining security controls. This guidance supports DoD system design, development, implementation, certification, and accreditation efforts.

### 1.4 Vulnerability Severity Code Definitions

Severity Category Codes (referred to as CAT) are a measure of risk used to assess a facility or system security posture. Each security policy specified in this document is assigned a Severity Code of CAT I, II, or III. Each policy is evaluated based on the probability of a realized threat occurring and the expected loss associated with an attack exploiting the resulting vulnerability.

**Table 1-1. Vulnerability Severity Category Code Definitions**

	<b>DISA/DIACAP Category Code Guidelines</b>	<b>Examples of DISA/DIACAP Category Code Guidelines</b>
CAT I	Any vulnerability, the exploitation of which will, directly and immediately result in loss of Confidentiality, Availability or Integrity. An ATO will not be granted while CAT I weaknesses are present.  Note: The exploitation of vulnerabilities must be evaluated at the level of the system or component being reviewed. A workstation for	Includes <b><u>BUT NOT LIMITED</u></b> to the following examples of direct and immediate loss:  1. May result in loss of life, loss of facilities, or equipment, which would result in mission failure. 2. Allows unauthorized access to security or administrator level resources or privileges. 3. Allows unauthorized disclosure of, or access to, classified data or materials. 4. Allows unauthorized access to classified facilities. 5. Allows denial of service or denial of access.

	DISA/DIACAP Category Code Guidelines	Examples of DISA/DIACAP Category Code Guidelines
	example, is a stand alone device for some purposes and part of a larger system for others. Risks to the device are first considered, then risks to the device in its environment, then risks presented by the device to the environment. All risk factors must be considered when developing mitigation strategies at the device and system level.	<p>which will result in mission failure.</p> <ol style="list-style-type: none"> <li>6. Prevents auditing or monitoring of cyber or physical environments.</li> <li>7. Operation of a system/capability which has not been approved by the appropriate Designated Accrediting Authority (DAA).</li> <li>8. Unsupported software where there is no documented acceptance of DAA risk.</li> </ol>
CAT II	<p>Any vulnerability, the exploitation of which, has a potential to result in loss of Confidentiality, Availability or Integrity. CAT II findings that have been satisfactorily mitigated will not prevent an ATO from being granted.</p> <p>Note: The exploitation of vulnerabilities must be evaluated at the level of the system or component being reviewed. A workstation for example, is a stand alone device for some purposes and part of a larger system for others. Risks to the device are first considered, then risks to the device in its environment, then risks presented by the device to the environment. All risk factors must be considered when developing mitigation strategies at the device and system level.</p>	<p>Includes <b><u>BUT NOT LIMITED</u></b> to the following examples that have a potential to result in loss:</p> <ol style="list-style-type: none"> <li>1. Allows access to information that could lead to a CAT I vulnerability.</li> <li>2. Could result in personal injury, damage to facilities, or equipment which would degrade the mission.</li> <li>3. Allows unauthorized access to user or application level system resources.</li> <li>4. Could result in the loss or compromise of sensitive information.</li> <li>5. Allows unauthorized access to Government or Contractor owned or leased facilities.</li> <li>6. May result in the disruption of system or network resources that degrades the ability to perform the mission.</li> <li>7. Prevents a timely recovery from an attack or system outage.</li> <li>8. Provides unauthorized disclosure of or access to unclassified sensitive, personally identifiable information (PII), or other data or materials.</li> </ol>
CAT III	Any vulnerability, the existence of which degrades measures to protect against loss of Confidentiality, Availability or Integrity. Assigned findings	<p>Includes <b><u>BUT NOT LIMITED</u></b> to the following examples that provide information which could potentially result in degradation of system information assurance measures or loss of data:</p> <ol style="list-style-type: none"> <li>1. Allows access to information that could lead</li> </ol>



	<b>DISA/DIACAP Category Code Guidelines</b>	<b>Examples of DISA/DIACAP Category Code Guidelines</b>
	<p>that may impact IA posture but are not required to be mitigated or corrected in order for an ATO to be granted.</p> <p>Note: The exploitation of vulnerabilities must be evaluated at the level of the system or component being reviewed. A workstation for example, is a stand alone device for some purposes and part of a larger system for others. Risks to the device are first considered, then risks to the device in its environment, then risks presented by the device to the environment. All risk factors must be considered when developing mitigation strategies at the device and system level.</p>	<p>to a CAT II vulnerability.</p> <ol style="list-style-type: none"> <li>2. Has the potential to affect the accuracy or reliability of data pertaining to personnel, resources, operations, or other sensitive information.</li> <li>3. Allows the running of any applications, services or protocols that do not support mission functions.</li> <li>4. Degrades a defense in depth systems security architecture.</li> <li>5. Degrades the timely recovery from an attack or system outage.</li> <li>6. Indicates inadequate security administration.</li> <li>7. System not documented in the sites C&amp;A Package/System Security Plan (SSP).</li> <li>8. Lack of document retention by the Information Assurance Manager (IAM) (i.e., completed user agreement forms).</li> </ol>

For wireless systems and devices, policies are classified as CAT I if failure to comply may lead to an exploitation which has a high probability of occurring, does not require specialized expertise or resources, and leads to unauthorized access to sensitive information (e.g., Classified). Exploitation of CAT I vulnerabilities allows an attacker physical or logical access to a protected asset, allows privileged access, bypasses the access control system, or allows access to high value assets (e.g., Classified).

Exploitation of CAT II vulnerabilities also leads to unauthorized access to high value information; however, additional sophistication, information, or multiple exploitations are needed. Exploitation of CAT II vulnerabilities provides information that have a high potential of allowing access to an intruder but requires one or more of the following: Exploitation of additional vulnerabilities, exceptional sophistication or expertise, or does not provide direct or indirect access to high value information (e.g., Classified).

A wireless policy with a CAT III severity code requires unusual expertise, additional information, multiple exploitations, and does not directly or indirectly result in access to high value information. Exploitation of CAT III vulnerabilities provides information that potentially could lead to compromise but requires additional information or multiple exploitations, and does not provide direct access to high value information (e.g., Classified).

## **1.5 STIG Distribution**

Parties within the DoD and Federal Government's computing environments can obtain the applicable STIG from the Information Assurance Support Environment (IASE) web site. This site contains the latest copies of any STIGs and Checklists, scripts, and other related security information. The Non-classified Internet Protocol Router Network (NIPRNet) Uniform Resource Locator (URL) for the IASE site is <http://iase.disa.mil/>.

## **1.6 Document Revisions**

Comments or proposed revisions to this document should be sent via e-mail to the following address: [fso\\_spt@disa.mil](mailto:fso_spt@disa.mil). DISA Field Security Operations (FSO) will coordinate all change requests with the relevant DoD organizations before inclusion in this document.

This page is intentionally left blank.

## **2. IPHONE AND IPAD DEVICE AND GOOD SERVER SECURITY INFORMATION**

Refer to the Good Technology iOS Hardening Guide for detailed information on security controls for DoD iOS 4 systems. GMS includes the Good for Enterprise (GFE) application client, the GFE Server, and the Mobile Control Server. GMS provides secure email, including Secure/Multipurpose Internet Mail Extensions (S/MIME) support; secure browsing via a DoD Internet proxy; Federal Information Processing Standard (FIPS) 140-2 data-at-rest encryption; plus a number of other security features. Email and security features of the GMS client are managed via the GMS servers, which are usually installed on the same network segment as the Exchange server. Note that GMS does not use ActiveSync to manage email.

### **2.1 Application Repository and Deployment**

The consumer model for deploying applications on iPhones is for the users to connect their devices online to the iTunes Store, purchase an application, and then download and install the application on the device. This model will not work in the DoD due to scalability issues, cost, and the need to tightly control the configuration of a DoD iPhone for security reasons.

In addition, the Apple model where agency-developed applications can only be deployed to iPhone and iPad users that are assigned to that agency will not work within the DoD unless all DoD-developed applications are signed and deployed by one DoD agency that acts as a DoD-wide iPhone application distribution center.

A DoD iPhone application distribution center should have the following features:

- Require Common Access Card (CAC)/Personal Identity Verification (PIV) card authentication for user access.
- Provide access to all DoD-approved commercial applications currently available on the iTunes Store and DoD-developed applications.
- Provide agencies/commands the capability to designate required/approved / not approved applications listed in the DoD iPhone application distribution center for assigned iPhone users.
- Restrict user access only to applications designated as approved or required by local commands, agencies, or Designated Approval Authorities (DAAs).
- Capability to purchase enterprise-wide licenses for applications available on the iTunes Store and host the application on the DoD application distribution center.
- Host DoD-developed applications.
- Provide a central distribution center where DoD iPhone users can connect new out-of-the-box devices to register devices and download all required software.
- Provide a central distribution center where DoD iPhone users can connect to download operating system patches.

Several DoD agencies are considering standing-up a DoD iPhone application distribution center but this capability is not expected to be available until early 2011, at the earliest. Therefore, application deployment capabilities in the DoD will be phased in with appropriate security controls implemented with each phase. Phase I of the DoD iPhone Application Distribution Process (current procedures) will include the following features:

- The site SA will set up and configure assigned iPhones.
- All approved commercial and DoD-developed applications will be loaded by the site SA during device provisioning or during a subsequent updates.
- Access to the iTunes Store will be disabled for individual iPhone users after the SA provisions the device.
- iPhones must be returned to the SA to have additional applications loaded on devices.

## 2.2 Provisioning Procedures

As described in Section 2.1, the ultimate goal is for DoD iPhone users to download all required software for new devices from a DoD iPhone application distribution center, but that capability is not currently available. Therefore, during Phase I of the DoD iPhone Application Distribution Process, site SAs will be responsible for provisioning site-managed iPhones using the procedures listed in Table 2-1.

**Table 2-1. Apple Device Provisioning Procedures**

STEP NUMBER	PROCEDURE
1	Install the GMS servers. See Appendix A for requirements.
2	Ensure the two required policy sets are set up on the GMS console: <ul style="list-style-type: none"> <li>- STIG Policy Set (Production)</li> <li>- STIG Policy Set (Provisioning/SW Updates)</li> </ul>
3	Add a user account in the GMS console for each device being provisioned. Assign the STIG Policy Set (Provisioning/SW Updates) to each account.
4	Download iTunes on a "provisioning" computer.
5	Set up a free iTunes account for each managed device.  To set up an iTunes account without entering a credit card number, launch iTunes on the provisioning personal computer (PC), click on "iTunes Store" in the left pane, click on "App Store" in the top bar, click on any "free" app and complete the registration process (recommend the GFE app be used). In the section where credit card information is entered, select "None." It is recommended a 15-character complex admin password that meets the requirements of CTO 07-15Rev1 be selected and the same password used for each site managed account. The password should be safeguarded using the same procedures as other SA passwords.
6	Activate each device via iTunes.
7	Download the GFE application from the iTunes Store to the device's iTunes account.
8	Download other DAA-approved commercial applications to the device iTunes account.  When applications are purchased in the iTunes Store, it is recommended that a pre-purchased iTunes card be used to purchase applications rather than

STEP NUMBER	PROCEDURE
	using a DoD credit card.
9	Install DoD-developed applications.  Follow instructions provided by the application developer.
10	Sync the iPhone with device's iTunes account.
11	Turn off the Bluetooth radio and Location Services.
12	Turn off the WiFi radio, if use is not approved.
13	Launch the Good client on the device.
14	Accept the request to receive notifications from Good, if received.
15	Enter the account email address and activation user PIN provided in the Good Management Console (GMC) when prompted.
16	Accept the prompt to download a device profile. The Good client will download the Good App configuration file. Click on "Install", and then click on "Install Now" after the profile has been downloaded.
17	The set up process will prompt you to enter a device unlock passcode. Enter a 3 character login passcode. (Note: if the passcode is not set as stated, the user may not be required to change the passcode in step 23 below.)
18	When the Root certificate install prompt is received, click on "Install Now."
19	After the setup process is completed, a "Password Required" box will pop up so the initial Good App password can be entered. Click "OK" twice and enter a 4 character Good App password. (Note: if the password is not set as stated, the user may not be required to change the password in step 23 below.)
20	Move the user account in the GMS console to the STIG Policy Set (Production).
21	Download and install the new policy set on the device.
22	Set up of the device is now complete.
23	Have users complete required training, document the user's completion or required training, and have users review and sign the User Agreement.
24	Give the device and initial device unlock passcode and Good App password to the user. The user will be prompted to change both after initial login.

### 2.3 Procedures For Changing Device Applications

During Phase I, site SAs should use the following procedures to add or remove applications on site managed devices, as provided in Table 2-2.

**Table 2-2. Apple Device Application Change Procedures**

STEP NUMBER	PROCEDURE
1	Users will return device to SA. Have the users provide their device passcode and Good App password to the SA.
2	Log into the user's iPhone. Remove the STIG profile.

STEP NUMBER	PROCEDURE
3	In the GMS console, move the user account to the STIG Policy Set (Provisioning/SW Updates) that allows the device to connect to iTunes and download applications.
4	Download and install the new profile on the device. Set the iPhone passcode to exactly 3 characters and the Good app password to exactly 4 characters. (Note: if the passcode and password are not set as stated, the user may not be required to change them in step 9 below.)
5	Connect the device to the device iTunes account and make changes to the device Apps List in iTunes.
6	Sync the device to iTunes.
7	In the GMS console, move the user account back to the STIG Policy Set (Production).
8	Download and install the new policy on the device.
9	Return the device to the user. Provide the user the new passcode and password. The user will be prompted to change both the device passcode and Good App password after initial login.

## 2.4 PKI Support

Procedures for downloading and installing DoD PKI certificates are found in Appendix C of this document.

### 2.4.1 S/MIME Configuration

S/MIME features are included in the GFE client that is installed on all DoD iPhones and iPads. Features will be deployed in the following four phases:

- S/MIME Lite
  - Verify certificate revocation status of digitally signed received email
- S/MIME Soft Token – (available September 2010, if approved by the Defense Information System Network (DISN) Security Accreditation Working [DSAWG]):
  - Verify status of digital signature for received email
  - Sign outgoing email using soft token
  - Encrypt outgoing email
  - Decrypt received email using soft token
- S/MIME – Hard Token (CAC) – (availability December 2010)
  - Verify status of digital signature for received email
  - Sign outgoing email using soft token
  - Encrypt outgoing email
  - Decrypt received email using soft token

- **Note:** The Bluetooth Smart Card Reader (SCR) must complete DoD Bluetooth validation testing before the Bluetooth connection can be used. Therefore, the SCR may be used initially with a wired connection to the iPhone.

#### 2.4.2 Using Software Certificates

DoD PKI-issued digital certificates are used to digitally sign and encrypt e-mails. When using PKI digital certificates with an iPhone, a user's digital certificates can be stored either on the handheld (software certificates) or on a CAC (hardware certificates). Software certificates are defined as any PKI certificate that does not require the presence of a CAC, smart card, or alternate hardware token for the certificate to be used for digital signature or encryption operations.

Software certificate use by end users must be approved by the Component DAA and remain in use only for the minimum time necessary to comply with the hardware token requirement. Approval of software certificate usage by the DAA can be for general use cases, for groups of individuals, or for organizations to preclude DAA's approving individual end-user instances of software certificate usage.

DoD is currently conducting a risk analysis on the use of both hardware- and software-based digital certificates on mobile devices to determine if current guidelines should be modified. It is not known when the results of this evaluation will be available.

#### 2.5 Remote Connections to DoD Networks

A Virtual Private Network (VPN) client is integrated with the iPhone operating system (OS 3.2 and iOS 4). The VPN client does not currently support CAC/PIV card authentication, use FIPS 140-2 validated encryption, or support CAC / PIV user authentication. Therefore, the VPN client cannot be used to set up a remote connection to a DoD network.

#### 2.6 Disposal of iPhone and iPad Devices

Appendix B provides required iPhone and iPad sanitization procedures to follow prior to disposing of the devices.

#### 2.7 Antivirus Support on iPhone and iPad Devices

DoDI 8500.2, Information Assurance (IA) Implementation, February 6, 2003, requires virus protection on mobile computing devices. In DoDI 8500.2, IA control ECVP-1 states: "All servers, workstations and mobile computing devices implement virus protection that includes a capability for automatic updates."

For some information technology (IT) systems, this requirement is met by using antivirus applications installed on the computer (e.g., IT systems with the Windows operating system). iPhone and iPad devices meet the virus protection requirement of DoDI 8500.2 by a combination of security policies, application control policies, and code signing to contain malware and control its ability to install itself on an iPhone or an iPad device and gain access to device resources, applications, and data and access the DoD network. This document includes specific GFE server and iPhone/iPad device configuration requirements to ensure malware controls are implemented.



iPhone virus protection features have been tested by the National Security Agency (NSA) and were approved by the Defense Information System Network (DISN) Security Accreditation Working Group (DSAWG) in (Month) 2010 as meeting DoD security requirements when the initial release of this STIG was approved. (**Note for Draft STIG:** this testing is ongoing as of 21 Sept 2010).

## 2.8 iPhone Instant Messaging (IM)

The Instant Messaging STIG provides security guidance on the use of IM applications in the DoD. DoD iPhone devices can be used to connect to any DoD-managed IM server or system that meets the requirements of the Instant Messaging STIG.

## 2.9 Enterprise Firewall Configuration

DoD security policy requires isolation of the GFE servers from the site's Internal Local Area Network (LAN) (also referred to as the Internal Enclave LAN) by installing a host-based firewall on the Windows host server or installing a firewall between the Windows server and the Internal Enclave LAN. The GFE server and Exchange servers must be placed on the same segment of the Internal Enclave LAN to facilitate communications. The GFE server also needs to communicate with other resources (such as e-mail servers, Lightweight Directory Access Protocol (LDAP) and Optical Supervisory Channel Protocol (OSCP) servers, authorized back-office web servers, Simple Object Access Protocol (SOAP) web services, and Java 2 Micro Edition (J2ME) applications) which may be located in various segments or security domains within the site's architecture. A DoD Host Based Security System (HBSS) firewall is acceptable in meeting this requirement.

The following information describes the configuration requirements of the host-based firewall located on the Windows server.

**Note:** It is the responsibility of each site's IAO to ensure required ports have been registered via the DoD Ports, Protocols, and Services Management (PPSM) process.

In general, the host-based firewall rules must be configured to implement the following policies:

- Internal traffic from the GFE server is limited to internal systems used to host the GFE services (e.g., e-mail, LDAP servers, and authorized back-office application and content servers). Communications with other services, clients, and/or servers are not authorized.
- Internet traffic from the GFE server is limited to only specified services (e.g., Good Network Operations Center (NOC), OSCP, Secure Sockets Layer (SSL)/Transport Layer Security (TLS), Hypertext Transfer Protocol (HTTP), and LDAP). All outbound connections are initiated by the GFE server.

Table 2-1 lists the default or standard ports, services, and Internet Protocol (IP) addresses for the needed services used for the GFE server. Although it is possible to configure Transmission Control Protocol (TCP) / User Datagram Protocol (UDP) to use non-standard or unregistered

ports for these communications, this is not recommended as it will cause unexpected results at various internal or external boundaries in the DoD enclave.

**Note:** Table 2-3 is intended as a starting point and is provided by request of field sites and reviewers to facilitate firewall configuration. Use additional references from Good Technology, Microsoft, and DISA STIGs to tailor the firewall rule configuration to the site's specific architecture.

**Table 2-3. Host-Based Firewall Architecture on GFE Server**

Service	Protocol	Default Port	Comments
Outgoing data connections to the Good NOC.	TCP	443	Both the Local Gateway Firewall and the Enclave Perimeter firewall outbound rules must be configured to allow this port outbound to Internet via NIPRNet.  (Must traverse Ports Protocols and Services (PPS) Category Assignment List (CAL) boundaries 12, 10, 6, 4, and 2 when configured in compliance with the requirements of this checklist.)
Outgoing connections to the Enclave web proxy server.	HTTP, Hypertext Transfer Protocol Secure (HTTPS)	8080, 8443	List IP address of the web proxy server in the host-based GFE server firewall list of trusted IP addresses and subnets.
Outgoing connections to Enclave application and content servers (e.g., J2ME servers, SOAP web services, and web content servers).	HTTP, HTTPS	8080, 8443	For approved/authorized connections to Internal Enclave application servers. The Firewall Administrator (FA) will update the host-based GFE server firewall rules to allow access, including listing IP address of the servers in the firewall list of trusted IP addresses and subnets.
Outgoing connection to trusted OCSP.	HTTP	80	To obtain PKI certificate information.
Outgoing LDAP connection	LDAP	389	
<b>For connections between the GFE Server and the Enclave Microsoft Exchange Server</b>			
Remote Procedure Call (RPC) endpoint mapper	TCP	135	
Microsoft Exchange System Attendant service	TCP	135	
Name Service Provider Interface (NSPI)	TCP	135	
Microsoft Exchange Information Store	TCP	135	

## **2.10 Wi-Fi Configuration**

Wi-Fi service is available on the iPhone, iPad, and iPod Touch devices. The Wi-Fi client is Wi-Fi Protected Access 2 (WPA2)-certified, but is not FIPS 140-2 validated and it does not support user authentication via CAC or PIV card.

The following subsections describe conditions that apply for Wi-Fi service use on DoD iOS devices.

### **2.10.1 Wi-Fi Connection to a DoD-Operated Enterprise WLAN System**

Connections to DoD-operated Enterprise Wireless Local Area Network (WLAN) access points that provide NIPRNet access are not authorized. Connections to DoD-operated WLAN access points that connect to only Internet gateways are authorized.

### **2.10.2 Wi-Fi Connection to a Public Hot Spot WLAN System**

Connections to public wireless hot spots and hotel hot spots are not authorized.

### **2.10.3 Wi-Fi Connection to a Home WLAN System**

Connections to home WLAN systems are authorized. Requirements for home Wi-Fi networks are included in the Apple iOS 4 STIG.

## **2.11 Bluetooth Configuration**

The iPhone Bluetooth radio stack does not meet DoD security requirements and therefore, must be disabled at all times.

## **2.12 Tethered Modem Use**

An iPhone<sup>1</sup> can be used as an “IP” modem or a “tethered modem” to provide a wireless Internet connection for a laptop computer. In some cases, this is less expensive than buying a broadband wireless card and setting up a separate broadband wireless account.

Note that most wireless carriers disable the capability for using the Safari browser to directly set up a tethered connection to a laptop via an Internet connection, thus forcing subscribers to buy a higher-priced “Tethered” service. Procedures for setting up IP modem service on a laptop are available from each wireless carrier.

---

<sup>1</sup> Tethered modem support for the iPad and the iPod Touch is not available.

## APPENDIX A. IOS DEVICE SYSTEM ADMINISTRATOR SECURITY CONFIGURATION TASKS

TASK #	TASK	REFERENCE	CHECK BOX WHEN TASK COMPLETED
1	Complete required SA training.	WIR-WMSP-001	
2	Install the GMS servers in the approved architecture.	WIR-WMS-GD-003	
3	Ensure the GMS servers are approved versions.	WIR-WMS-GD-001	
4	Ensure the GFE Windows server is STIG compliant. Run the appropriate Windows Server Gold Disk.	WIR-WMS-GD-002	
5	Ensure the GFE server is Structured Query Language (SQL) and Apache Tomcat STIG compliant.	WIR-WMS-GD-002	
6	Configure the host-based firewall on the GFE server.	WIR-WMS-GD-004	
7	Set up two STIG-compliant security policy sets on the GFE server: Production and Provisioning / SW Updates.	WIR-WMS-GD-007	
8	Assign all user accounts to a STIG-compliant Production security policy set. Follow recommended device provisioning procedures.	WIR-WMS-GD-007 Sections 2.2 and 2.3	
9	Determine what iPhone applications are approved via the site application approval process.	WIR-MOS-iOS-006	
10	If connections to back-office servers are allowed for iPhone users, configure the GMS host-based firewall for access and configure CAC authentication on back-office servers. (Future capability)	WIR-WMS-GD-005-01 WIR-WMS-GD-005-02	
11	Block HTML/Rich Text Format (RTF) e-mail format on the GFE server. (Done automatically by Good server. Future server update will allow active content in email so this feature must be disabled at that time.)	WIR-WMS-GD-006	
12	Set up alerts when user activates Bluetooth and WiFi radios. (Future capability)	WIR-GMMS-007	
13	Set up SA accounts with authorized roles in Good console.	WIR-WMS-GD-008	

<b>TASK #</b>	<b>TASK</b>	<b>REFERENCE</b>	<b>CHECK BOX WHEN TASK COMPLETED</b>
14	Configure S/MIME features on the GFE server.	Appendix C, Apple iOS 4 Technology Overview	
15	Perform an annual security self assessment on the GMS server.	DoD Policy	

## APPENDIX B. IPHONE AND IPAD DISPOSAL PROCEDURES

### **Detailed Procedures for Sanitizing DoD iPhone and iPad Devices Prior to Disposal<sup>2</sup>**

1. On the iPhone/iPad, select "Settings"
2. Select "General"
3. Select "Reset"
4. Select "Erase All Content and Settings"
5. Select "Erase iPhone" or "Erase iPad"

These procedures should be used prior to transferring iPhones from current users to new users or before disposing of old devices via site property disposal procedures.

---

<sup>2</sup> This procedure assumes no classified information is on the iOS device. This procedure should not be used for sanitizing iOS devices after a Classified Message Incident (CMI).

This page is intentionally left blank.

## APPENDIX C. GOOD MOBILE CONTROL AND END USER S/MIME CONFIGURATION

### C.1 Run InstallRoot on Good Mobile Control (GMC) Server

The DoD Root and Intermediate Certificate Authorities, must be installed in the GMC server's local computer store for S/MIME operations to work successfully. InstallRoot can be obtained from <http://iase.disa.mil/pki-pke/index.html> or <http://www.dodpke.com>.

**Critical Information:** The DoD issues new intermediate CAs once a year so GMC server administrators must check for new releases of InstallRoot. If the GMC server does not have up to-date intermediate CAs, users will not be able to verify signatures of users with credentials issued from newer CAs. A notice is sent out in a CYBERCOM Info Spot when new intermediate CAs are issued.

### C.2 Obtain SSL Certificate for GMC Server

An SSL certificate must be requested from the local organization's Registration Authority and installed on the GMC server. Please refer to <http://iase.disa.mil/pki-pke/index.html> or contact [pke\\_support@disa.mil](mailto:pke_support@disa.mil) for instructions to request an SSL certificate for the appropriate operating system that is installed on the GMC server.

### C.3 Configure GMC Server to use DoD SSL Certificate

The GMC server is initially configured to use a self-signed certificate. Once the DoD SSL certificate is installed on the GMC server, export it from the key store in the PKCS#12 format (.pfx extension by default) following password complexity guidelines for software certificates (as defined in CYBERCOM CTO 07-015Rev1) and copy it to the GMC tomcat directory (C:\Program Files\Good Technology\Good Mobile Control\tomcat). Then modify the config.props file located in the GMC directory (C:\Program Files\Good Technology\Good Mobile Control) as shown below:

Change the underlined entries

```
#### Configuration for embedded web server
#
# console.http.port                8080
# console.https.port              8443
# console.localhost
# console.context.path
# console.context.docBase          emf
# console.keystore.file            emf_cert.p12
# console.keystore.password       changeit
# console.keystore.type           PKCS12
```

To match the following (be sure to remove the '#' at the front of the line)



### ### Configuration for embedded web server

```
#
# console.http.port          8080
# console.https.port        8443
# console.localhost
# console.context.path
# console.context.docBase   emf
console.keystore.file        myDoDSSLcert.pfx
console.keystore.password    mypassword
console.keystore.type        PKCS12
```

**Critical Information:** USCYBERCOM CTO 07-015 Revision 1, PKI Implementation Phase 2 (Task 4 sub-bullet 3) states the removal of software certificate installation files does not apply to Server based applications that have a requirement for PKCS#12 certificate files.

## C.4 Server Configuration

S/MIME must first be enabled by a Good Technology Engineer at the Good NOC before you can proceed with configuration. Port 80 and 389 must be open outbound on the local enclave firewall from the GMC server to \*.disa.mil for S/MIME to work. Verify this information prior to proceeding (there may be more than one firewall between the GMC server and \*.disa.mil service offerings) by performing the following steps:

1. Log into the GMC web interface using the Good Administrator account (e.g. GoodAdmin) established during installation.
2. Click the **Settings** tab at the top of the screen.
3. Select **Secure Messaging (S/MIME)** from the left column.
4. Enter the following **bold** information exactly as shown in Figure C-1:

#### Certificate Authorities Directory (LDAP)

Host: **crl.gds.disa.mil**

Port: **389**

Base: **ou=PKI,ou=DoD,o=U.S. Government,c=US**

#### User Certificate Directory (LDAP)

Host: **dod411.gds.disa.mil**

Port: **389**

Base: **ou=PKI,ou=DoD,o=U.S. Government,c=US**

#### OCSP Responder

URL: **http://ocsp.disa.mil**

**Critical Information:** A DoD component CANNOT verify signatures from a non-DoD organization without configuring a local enclave OCSP responder. Contact the local network administrators for availability of a local OCSP responder.

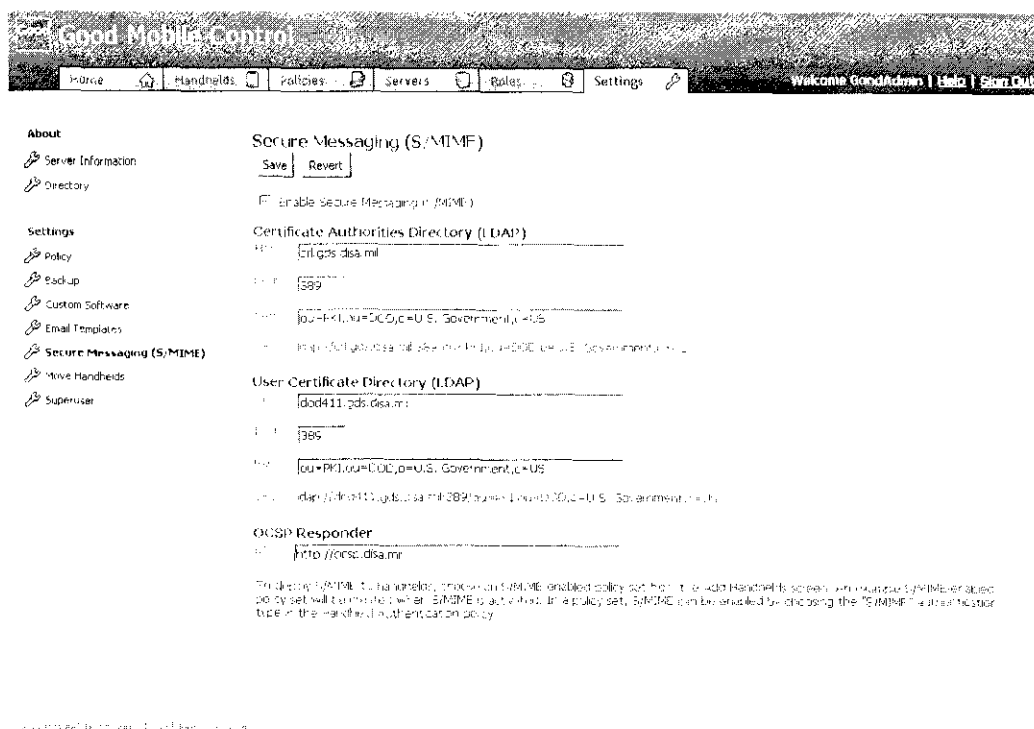


Figure C-1. S/MIME Server Configuration

## C.5 Initial User Configuration

Users who will utilize S/MIME on their devices must have a handheld in an S/MIME-enabled policy and be added to GMC as the **Self Service** role by performing the following steps:

1. Log into the GMC web interface using the Good Administrator account (e.g. GoodAdmin) established during installation.
2. Click the **Roles** tab at the top of the screen.
3. Select **Self Service** from the left column.
4. Click the **Add** button under Members.
5. In the **Look For** field enter the users name and click **Look Now**.
6. Click the users name in the **Search Result** field and it will automatically move the user into the **Add these members** field.
7. You can add multiple users by repeating steps 5-6 or you can add an Active Directory Group that contains all the S/MIME users.
8. Click the **Add** button to complete the process.

### Software Certificates

After the user's device has been provisioned (awaiting password entry to continue Good App installation) and he/she has been added as the Self Service role on GMC, his/her device can be configured to use software certificates for S/MIME operations. **During installation of the iOS Good App on the device, the user is going to be asked to provide his/her email digital signature and decryption software certificates.**

**Note:** Software certificates are not currently supported on the iOS Good App so these steps may be slightly different when the final product is released.

1. Users must log into the GMC web interface from their desktop using their Active Directory credentials (**Note:** Good Technology needs to add smart card logon for GMC).
2. Users will be presented with their self service portals as shown in Figure C-2.



**Figure C-2. Good Mobile Control Self Service Portal**

3. Users must press the software certificates button and they will be asked to select one .p12 or .pfx file for their digital signature and a second for email decryption (**Note:** This will be added to the graphical user interface [GUI]).
4. The users' private keys will be sent through the FIPS 140-2 validated tunnel to their devices over-the-air and the installation of the iOS Good App will continue.

### Smart Cards

After the user's device has been provisioned (awaiting password entry to continue Good App installation) and his/her have been added as the Self Service role on GMC his/her device can then be configured to use his/her smart card for S/MIME operations. **During installation of the iOS Good App on the device, the user is going to be asked to connect his/her smart card reader (SCR) and import the smart card certificates (pointers to the private keys stored on the smartcard).** **Note:** There is not currently an approved iOS-compatible SCR and hardware certificates are not currently supported on the iOS Good App, so these steps may be different when the final product is released.

1. When prompted during installation of the iOS Good App, the user must connect their iOS-compatible SCR to their devices (without their smart card inserted).

2. Once connection is successful, the users must insert their smart cards into the reader and they must enter their smart card PIN when prompted.
3. This will import the users' smart card certificates and installation of the iOS Good App will continue.

### **C.6 Setup Procedure When User Is Issued New Credentials (Or Loss of SCR)**

When a user is issued new tokens, first ensure that he/she has a back up of the email decryption private key. Contact the local registration authority or visit <http://iase.disa.mil/pki-pke/index.html> for guidance on backing up a users email decryption private key.

#### **New Software Certificates**

From the iOS device, the user must go into the settings in his/her iOS Good App and select update credentials. They will be prompted to log into the GMC self service portal and follow the same steps as initial Software Certificate provisioning.

#### **New Smart Card or New SCR**

From the iOS device, the user must go into the settings in his/her iOS Good App and select CAC/PIV setup. He/she will then be prompted to connect their SCR and import their smart card certificates following the same steps as initial smart card provisioning.

For additional information or assistance on iPhone/iPad PKI issues, contact the DoD PKE office at [pke\\_support@disa.mil](mailto:pke_support@disa.mil) or visit their web site at <https://www.us.army.mil/suite/page/474113>.

This page is intentionally left blank.

## APPENDIX D. VMS PROCEDURES

The following information applies only to teams and sites that use Vulnerability Management System (VMS) to enter and track DoD assets. When conducting an iOS device (iPhone, iPad, or iPod Touch) SRR, the Team Lead and the assigned Reviewer identify security deficiencies and provide data from which to predict the effectiveness of proposed or implemented security measures associated with the iPhone/iPad system and operating environment.

Both the Reviewer and the SA will create, maintain, and track assets in VMS. The Reviewer will use the Asset and Finding Maintenance screen to perform these functions. The SA will use the By Location navigation chain to perform the same function. When Reviewers access the Asset and Finding Maintenance screen, the Navigation pane displays a white Visits folder. Expand this Visits folder to display its subfolders. Each subfolder represents an individual visit in VMS that is assigned for review. Click (+) to expand the visit and display the location summaries for the visit. Within the location, iPhone and iPad assets are tracked using the Computing and Non-Computing asset types.

Use the following VMS Asset Matrix to select the appropriate asset type for each iPhone, iPad, or iPod Touch asset. The Reviewer or the SA must enter the entire asset posture including non-wireless related applications and services installed on the GFE server.

VMS Asset Matrix		
Wireless Technology	VMS Asset Type	ASSET POSTURE
Good Mobility Suite (GMS) Server Policies  A non-computing asset is created at the site where the GMS is installed so that all policy requirements can be applied to the site.	Non-Computing	The site admin or reviewer should create one non-computing asset for the GMS server system at the site. An example asset name to use may be: Site Q Good Mobility Suite Server  After creating the asset, the following postures should be applied to the asset:  <b>Non-Computing &gt; Policy &gt; Network Policy Requirements &gt; Wireless &gt; <i>General Wireless Policy</i></b>  <b>Non-Computing &gt; Policy &gt; Application Policy &gt; <i>Wireless Management Server Policy</i></b>

<b>VMS Asset Matrix</b>		
<b>Wireless Technology</b>	<b>VMS Asset Type</b>	<b>ASSET POSTURE</b>
<p>Apple iOS 4 Device Policies</p> <p>A non-computing asset is created at the site where the Apple iOS devices are issued and managed so that all policy requirements can be applied to the site.</p>	Non-Computing	<p>The site admin or reviewer should create one non-computing asset for the Apple iOS devices managed by the site. An example asset name to use may be: Site Q iPhone/iPad Devices</p> <p>After creating the asset, the following postures should be applied to the asset:</p> <p><b>Non-Computing &gt; Policy &gt; Network Policy Requirements &gt; Wireless &gt; <i>General Wireless Policy</i></b></p> <p><b>Non-Computing &gt; Policy &gt; Network Policy &gt; Wireless Policy &gt; <i>Smartphone Handheld Policy</i></b></p>
<p>GMS Servers</p> <p><b>Note:</b> Only configure asset for applications installed on the <b>same</b> server as the GFE application. There are no checks for LDAP.</p>	Computing	<p><b>Computing &gt; Operating System</b> – Windows. Expand and select version, then service pack installed.</p> <p><b>Computing &gt; Application &gt; Wireless Management Server &gt; <i>Good Mobile Messaging Server</i></b></p> <p>Select the following role: <b>Computing &gt; Role &gt; Wireless Role &gt; Wireless Management Srv &gt; <i>Apple iOS</i></b></p> <p><b>Application</b> – SQL  <b>Application</b> – Apache Web Server  <b>Application</b> – Antivirus. Expand and select version.  <b>Application</b> – Expand and select other applications installed on the same server to capture the entire asset posture of the server (e.g., Internet Information Services (IIS), Exchange, Browsers, Office Automation, etc).</p> <p><b>Role</b> – Member Server</p>

VMS Asset Matrix		
Wireless Technology	VMS Asset Type	ASSET POSTURE
Apple iPhone	Computing	<p><b>Note:</b> Do not mark as a workstation.  <b>Note:</b> Do not enter IP or Media Access Control address.</p> <p><b>Computing &gt; Operating System &gt; Mobile OS &gt; Apple &gt; Apple iOS 4</b></p> <p>Select the following role: <b>Computing &gt; Role &gt; Wireless Role &gt; Wireless Management Client &gt; Good Mobile Messaging</b></p>
Apple iPad	Computing	<p><b>Note:</b> Do not mark as a workstation.  <b>Note:</b> Do not enter IP or Media Access Control address.</p> <p><b>Computing &gt; Operating System &gt; Mobile OS &gt; Apple &gt; Apple iOS 4</b> (Note: use this posture for OS 3.2 also.)</p> <p>Select the following role: <b>Computing &gt; Role &gt; Wireless Role &gt; Wireless Management Client &gt; Good Mobile Messaging</b></p>
Apple iPod Touch	Computing	<p><b>Note:</b> Do not mark as a workstation.  <b>Note:</b> Do not enter IP or Media Access Control address.</p> <p>Select the following role: <b>Computing &gt; Role &gt; Wireless Role &gt; Wireless Management Client &gt; Good Mobile Messaging</b></p> <p>Select the following role when prompted: <b>Good Mobile Messaging</b></p>



This page is intentionally left blank.

UNCLASSIFIED

**iPhone / iPad STIG Check Cross Reference Table – Check to  
Asset  
21 September 2010**

STIG ID #	VMS #	Vulnerability	Apple iOS 4 Handheld Device	Good Mobility Suite Server
<b>General Wireless Policy Checks (Non-Computing)</b>				
WIR0005	V0008283	Only authorized wireless systems used	✓	✓
WIR0010	V0015782	Personally owned PEDs are used	✓	✓
WIR0015	V0008284	Site maintains equipment list for PEDs	✓	✓
WIR0020	V0008297	SSP includes wireless systems / equipment	✓	✓
WIR0025	V0014894	Wireless devices are physically secured	✓	✓
WIR0030	V0013982	Sign User Agreement	✓	✓
WIR0035	V0012072	Wireless devices in SCIFs are DCID / ICD compliant	✓	✓
WIR0040	V0012106	CTTA coordination for classified wireless	✓	✓
WIR0045	V0019813	No embedded wireless NIC on classified computers	✓	✓
<b>Smartphone Policy Checks (Non-Computing)</b>				
WIR-SPP-001	V0024953	Site PED/Smartphone camera policy	✓	
WIR-SPP-002	V0024954	PEDs with cameras not allowed in classified areas	✓	
WIR-SPP-003-01	V0024955	Publish CMI procedures for smartphones	✓	✓
WIR-SPP-003-02	V0024957	Site must follow required CMI procedures	✓	✓
WIR-SPP-004	V0024958	Follow procedures for disposal of smartphones	✓	
WIR-SPP-005	V0024960	Do not use smartphone for classified data	✓	
WIR-SPP-006	V0024961	Smartphone users receive required training	✓	
WIR-SPP-007-01	V0024962	Publish lost / stolen smartphone procedures	✓	✓
WIR-SPP-007-02	V0024969	Follow lost / stolen smartphone procedures	✓	✓
WIR-SPP-008-01	V0024963	Smartphone provisioning -01	✓	
WIR-SPP-008-02	V0024964	Smartphone provisioning -02	✓	
WIR-SPP-009	V0024965	Instant Messaging (IM)	✓	
WIR-SPP-010	V0024966	Smartphone WiFi policy	✓	
WIR-SPP-011	V0024968	Use of software certificates approved	✓	
<b>Wireless Management Server Policy Checks (Non-Computing)</b>				
WIR-WMSP-001	V0024970	Smartphone admin training		✓
WIR-WMSP-002	V0024971	Annual self assessments		✓
<b>Wireless Remote Access Policy Checks (Non-Computing)</b>				
WIR-WRA-001	V0025034	Complete user training for wireless remote access	✓	
WIR-WRA-002	V0025035	Site has wireless remote access policy	✓	
WIR-WRA-003	V0025036	Wireless remote access included in SSP	✓	
<b>Good Mobility Suite Server Checks (Computing)</b>				
WIR-GMMS-001	V0024987	Re-challenge for CAC PIN		✓

UNCLASSIFIED

## UNCLASSIFIED

STIG ID #	VMS #	Vulnerability	Apple iOS 4 Handheld Device	Good Mobility Suite Server
WIR-GMMS-002	V0024995	Screen capture		✓
WIR-GMMS-003	V0024998	Expire OTA PIN		✓
WIR-GMMS-004	V0024999	Do not allow OTA Provisioning PIN reuse		✓
WIR-GMMS-005	V0025000	Enable iPhone Configuration		✓
WIR-GMMS-006-01	V0025002	iOS compliance check - device hardware version		✓
WIR-GMMS-006-02	V0025003	iOS compliance check - device iOS version		✓
WIR-GMMS-006-03	V0025004	iOS compliance check -device jailbreak detection		✓
WIR-GMMS-006-04	V0025005	iOS compliance check - Good iOS client		✓
WIR-GMMS-007	V0025023	Bluetooth/WiFi Alert		✓
WIR-GMMS-008	V0025028	Password / passcode reset		✓
WIR-GMMS-010-01	V0025032	Enable password access to Good app		✓
WIR-GMMS-010-02	V0025030	Contacts synchronization		✓
WIR-WMS-GD-001	V0024972	Required smartphone management server version used		✓
WIR-WMS-GD-002	V0024973	Smartphone management server STIG compliant		✓
WIR-WMS-GD-003	V0024974	Smartphone management server architecture		✓
WIR-WMS-GD-004	V0024975	Configure smartphone management server firewall		✓
WIR-WMS-GD-005-01	V0024976	Connections to back-office servers		✓
WIR-WMS-GD-005-02	V0024980	Connections to back-office servers		✓
WIR-WMS-GD-006	V0024977	Block HTML / RTF email		✓
WIR-WMS-GD-007	V0024978	User accounts assigned to STIG compliant policy		✓
WIR-WMS-GD-008	V0024979	Smartphone server authentication		✓
WIR-WMS-GD-009-01	V0024988	Set handheld password to expire as required		✓
WIR-WMS-GD-009-02	V0024989	Disallow previously used passwords		✓
WIR-WMS-GD-009-03	V0024990	Password minimum length		✓

UNCLASSIFIED

## UNCLASSIFIED

STIG ID #	VMS #	Vulnerability	Apple iOS 4 Handheld Device	Good Mobility Suite Server
WIR-WMS-GD-009-04	V0024991	Disallow repeated password characters		✓
WIR-WMS-GD-009-05	V0024994	Lock handheld when idle		✓
WIR-WMS-GD-009-06	V0024992	Maximum invalid password attempts		✓
WIR-WMS-GD-009-07	V0024993	Wipe handheld data after maximum password attempts		✓
<b>Apple iOS 4 Checks (Computing)</b>				
WIR-iOS-001	V0025019	iOS Bluetooth	✓	
WIR-iOS-002	V0025020	iOS WiFi	✓	
WIR-iOS-003	V0025021	iOS OS updates	✓	
WIR-iOS-004	V0025051	Location services	✓	
WIR-iOS-005	V0025092	WiFi - Ask to Join Networks	✓	
WIR-iOS-006	V0025093	Safari - AutoFill	✓	
WIR-MOS-iOS-001	V0024981	Use approved smartphone software versions	✓	
WIR-MOS-iOS-002	V0024982	Use approved SCR software version	✓	
WIR-MOS-iOS-003	V0024983	S/MIME installed on smartphone	✓	
WIR-MOS-iOS-004	V0024984	User auto-signature on email	✓	
WIR-MOS-iOS-005	V0024985	Use DoD Internet proxy	✓	
WIR-MOS-iOS-006	V0024986	Smartphone Apps approved	✓	
WIR-MOS-iOS-007	V0025022	Required logon banner	✓	
WIR-MOS-iOS-G-008	V0025001	Enable remote full device wipe	✓	
WIR-MOS-iOS-G-009	V0025006	Require password to remove profile	✓	
WIR-MOS-iOS-G-010	V0025007	Require passcode	✓	
WIR-MOS-iOS-G-011	V0025016	Minimum passcode length	✓	
WIR-MOS-iOS-G-012	V0025008	Password complexity	✓	
WIR-MOS-iOS-G-013	V0025009	Maximum passcode age	✓	

UNCLASSIFIED

## UNCLASSIFIED

STIG ID #	VMS #	Vulnerability	Apple iOS 4 Handheld Device	Good Mobility Suite Server
WIR-MOS-iOS-G-014	V0025017	Apple iOS device Autolock	✓	
WIR-MOS-iOS-G-015	V0025018	Smartphone passcode history	✓	
WIR-MOS-iOS-G-016	V0025010	Smartphone inactivity timeout	✓	
WIR-MOS-iOS-G-017	V0025011	iPhone passcode maximum failed attempts	✓	
WIR-MOS-iOS-G-018	V0025033	iOS Safari	✓	
WIR-MOS-iOS-G-019	V0025012	Public application store	✓	
WIR-MOS-iOS-G-020	V0025013	Smartphone application installation	✓	
WIR-MOS-iOS-G-021	V0025014	Smartphone camera	✓	
WIR-MOS-iOS-G-022	V0025015	iPhone screen capture	✓	
TBD	TBD	Game Center	✓	
WIR0925	V0018630	Separate DoD residential WLAN for DoD computer	✓	
WIR0930	V0018631	Home WLAN access point security	✓	
WIR0935	V0018747	Change DoD Residential WLAN SSID default	✓	
WIR0940	V0018748	DoD residential WLAN wireless router	✓	

UNCLASSIFIED

**DRAFT**

# **Apple iOS with Good Mobility Suite Configuration Tables**

Version 1, Release 0.1

21 September 2010

**LIST OF TABLES**

	<b>Page</b>
Table 1. Good Mobility Suite Server Configuration Settings.....	3
Table 2. iOS 4 Device User Based Enforcement Settings .....	12
Table 3. List of Core iOS 4 Applications .....	14

**NOTE:** In Table 1, “Required” settings must be implemented by all DoD iOS / Good Mobility Suite systems. “Optional” settings are recommended settings and may be changed to meet mission requirements.

**Table 1. Good Mobility Suite Server Configuration Settings**

Policy Rule	Setting		Comments	Good iOS Hardening Guide Reference #	STIG ID #	VMS #
	Required	Optional				
General Server Settings						
User enabled Bluetooth Radio Alert	Enable		Feature not yet available. Expected availability: September 2010		WIR-GMMS-007	V0025023
User enabled WiFi Radio Alert	Enable		Feature not yet available. Expected availability: September 2010		WIR-GMMS-007	V0025023
Password / Passcode rest after initial login			No configuration required. Automatically enabled by the Good server when the user is switched from the Provisioning Policy Set to the Production Policy Set		WIR-GMMS-008	V0025028
Connections to back office servers enabled			Feature not yet available. Expected availability: December 2010		WIR-WMS-GD-005-01 and WIR-WMS-GD-005-02	V0024976 and V0024980
Block HTML / RTF email, convert to text	Automatically enabled by the Good server		No configuration required. A future release of the Good server will support Hypertext Markup Language (HTML.) in email. When this capability is released, the feature will then be configured to convert active content to text.		WIR-WMS-GD-006	V0024977
Auto-signature configuration		Disable on server	See the Good iOS Hardening Guide for instructions (Section 3.3, Step 29).			
Enable secure browser	Enable		Feature not yet available. Expected availability: Sept 2010		WIR-MOS-iOS-005	V0024985



Policy Rule	Setting		Comments	Good iOS Hardening Guide Reference #	STIG ID #	VMS #
	Required	Optional				
Logon Banner	Enable		Feature not yet available. Expected availability: September 2010  Banner must have the following test: "I've read and consent to terms in IS user agreem't."		WIR-MOS-iOS-007	V0025022
CAC authentication for Good console admin accounts	Enable		Feature not yet available. Expected availability: December 2010		WIR-WMS-GD-008	V0024979
<b>STIG Policy Set Settings</b>						
<b>Handheld Section</b>						
Handheld Authentication Type	S/MIME with a password-protected lock screen or CAC PIN (Enables S/MIME)			GMC-01-01	WIR-GMMS-010-01	V0025032
<b>S/MIME with Password-protected lock screen or CAC PIN</b>						
Authenticate with CAC PIN		Do not check				
Authenticate with password		Check				
Re-challenge for CAC PIN every	Check  Set for 60 minutes or less		Recommended setting is 15 minutes.	GMC-01-02	WIR-GMMS-001	V0024987
Digitally sign all outgoing email		Do not check				
Encrypt contents and attachments of all outgoing mail		Do not check				
<b>Password Authentication</b>						
Expire password after	90 days or less			GMC-01-03	WIR-WMS-GD-009-01	V0024988
Disallow previously used passwords	3 or more			GMC-01-04	WIR-WMS-GD-009-02	V0024989

Policy Rule	Setting		Comments	Good iOS Hardening Guide Reference #	STIG ID #	VMS #
	Required	Optional				
Require minimum length of	8 or more  4		Use eight (8) or more for the Production Policy Set  Use exactly four (4) for the Provisioning / SW Update Policy Set.	GMC-01-05	WIR-WMS-GD-009-03	V0024990
Disallow repeated characters after	Select either 1 or 2		More than 2 repeated characters not allowed.	GMC-01-06	WIR-WMS-GD-009-04	V0024991
Require both letters and numbers		Do not check				
Require both upper and lower case		Do not check				
Require at least one special character		Do not check				
Do not allow sequential numbers		Do not check				
Do not allow personal information		Do not check	This feature is not supported on iOS devices.			
Do not allow more than one password change per day		Do not check				
<b>Lock Screen Protection</b>						
Require password when screen idle for more than	Select 15 minutes or less			GMC-01-07	WIR-WMS-GD-009-05	V0024994
For iPhone, always require password on application startup		Do not check				
After ___ invalid password attempts	Check Select 10 or less			GMC-01-09	WIR-WMS-GD-009-06	V0024992
Lock out user	Do not check					
Wipe handheld data	Check			GMC-01-10	WIR-WMS-GD-009-07	V0024993
Show notifications on lock screen		Do not check				

Policy Rule	Setting		Comments	Good iOS Hardening Guide Reference #	STIG ID #	VMS #
	Required	Optional				
Allow access to Good Contacts (numbers only) during dialing		Do not check	This feature is not applicable to iOS devices.			
<b>Messaging Section</b>						
<b>Good Mobile News</b>						
Enable Good Mobile News (RSS)		Do not check	This feature is not applicable to iOS devices.			
Email		Use all defaults				
Sending Attachments		Use all defaults				
<b>Copy and Paste</b>						
Do not allow data to be copied from the good application	Check			GMC-02-01	WIR-GMMS-002	V0024995
<b>Contacts</b>						
Enable access to Good Contacts		Check	Contact synchronization must also be enabled in the Good App (Preferences > Contacts > Sync with Handheld) for Good contacts to synchronize with iPhone Contacts.	GMC-02-02	WIR-GMMS-010-02	V0025030
Choose Fields	Choose only defaults, if checked.		Defaults: first name, last name, phone numbers	GMC-02-02	WIR-GMMS-010-02	V0025030
Enable Exchange Global Address List lookup		Check				
Enable access to public folders		Do not check	This feature is not supported on iOS devices.			
Allow contact beaming		Do not check	This feature is not applicable to iOS devices.			
Receiving Attachments		Use all defaults				
<b>Network Communications Section (see the Good iOS Hardening Guide)</b>						
<b>Provisioning Section</b>						
<b>OTA Provisioning PIN</b>						

Policy Rule	Setting		Comments	Good iOS Hardening Guide Reference #	STIG ID #	VMS #
	Required	Optional				
OTA Provisioning PIN expires after	Check 7 days or less			GMC-04-01	WIR-GMMS-003	V0024998
Allow OTA Provisioning PIN reuse	Do not check			GMC-04-02	WIR-GMMS-004	V0024999
Welcome email			Use defaults			
<b>Storage Card Section (see the Good iOS Hardening Guide)</b>						
<b>Blocked Application Section (see the Good iOS Hardening Guide)</b>						
<b>Compliance Manager Section (see the Good iOS Hardening Guide)</b>						
iOS Hardware Verification rule	Select configurations shown in Comments.		-Check to run: iOS Hardware Verification -Conditions: iPhone 3GS, iPhone 4, iPad, iPod Touch 3 <sup>rd</sup> generation -Failure Action = Wipe Enterprise Data -Check Every – 1 hour		WIR-GMMS-006-01	V0025002
OS Version Verification	Select configurations shown in Comments.		-Check to run: OS Version Verification -Conditions: 3.2.2, 4.1 (3.2.2 is allowed only until iOS 4 is released for the iPad) -Failure Action = Wipe Enterprise Data -Check Every – 1 hour		WIR-GMMS-006-02	V0025003
iOS Jailbreak Detection	Select configurations shown in Comments.		-Check to run: Jailbreak/Rooted Detection -Failure Action = Wipe Enterprise Data -Check Every – 1 hour		WIR-GMMS-006-03	V0025004

Policy Rule	Setting		Comments	Good iOS Hardening Guide Reference #	STIG ID #	VMS #
	Required	Optional				
iOS Client Version Verification rule	Select configurations shown in Comments.		-Check to run: iOS Client Version -Good for Enterprise version must be at least: 1.6.1 -Failure Action – Wipe Enterprise Data -Check Every = 1 hour		WIR-GMMS-006-04	V0025005
<b>Data Encryption Section (see the Good iOS Hardening Guide)</b>						
<b>Software Deployment Section (see the Good iOS Hardening Guide)</b>						
<b>Good Mobile Access Section (see the Good iOS Hardening Guide)</b>						
<b>iPhone Configuration Section</b>						
<b>General Tab</b>						
Enable iPhone Configuration	Check		Enter profile name and organization	GMC-11-01	WIR-GMMS-005	V002500
Enable remote full device wipe	Check			GMC-11-02	WIR-MOS-iOS-G-008	V0025001
<b>Profile Security</b>						
Allow user to remove profile	Do not check					
Require password to remove profile	Check		Set password to complex 15 characters in accordance with CYBERCOM Communications Tasking Order ( CTO) 07-15Rev1	GMC-11-03	WIR-MOS-iOS-G-009	V0025006
Do not allow profile to be removed		Do not check				
<b>Passcode Tab</b>						
Require passcode	Check			GMC-11-04	WIR-MOS-iOS-G-010	V0025007
Minimum length of	4 or more  3		Use 4 or more for the Production Policy Set  Use exactly 3 for the Provisioning / SW Update Policy Set.	GMC-11-04	WIR-MOS-iOS-G-011	V0025016

Policy Rule	Setting		Comments	Good iOS Hardening Guide Reference #	STIG ID #	VMS #
	Required	Optional				
Allow simple value	Check			GMC-11-05	WIR-MOS-iOS-G-012	V0025008
Alphanumeric		Do not check				
Minimum number of complex characters		Do not check				
Maximum passcode age	90 days or less			GMC-11-06	WIR-MOS-iOS-G-013	V0025009
Auto-lock	Check Set at 5 minutes or less		5 minutes is the max setting allowed in iOS 4	GMC-11-07	WIR-MOS-iOS-G-014	V0025017
Passcode history	3 or more			GMC-11-08	WIR-MOS-iOS-G-015	V0025018
Grace Period	Check Set for 15 minutes or less		Note: if the user does not change the passcode setting under Settings > General > Passcode Lock > Require Passcode from "Immediately" to "After 15 minutes," the screen will lock as soon as the Auto-lock feature forces the screen to go blank.	GMC-11-09	WIR-MOS-iOS-G-016	V0025010
Maximum failed attempts	Check Set to 10 or less			GMC-11-10	WIR-MOS-iOS-G-017	V0025011
<b>Restrictions Tab</b>						
Allow explicit content		Do not check	Note: this feature only blocks access to the explicit content on the iTunes Music Store web site.	GMC-11-11		
Allow use of Safari	Check		Required by the Good App.	GMC-11-12	WIR-MOS-iOS-G-018	V0025033
Allow use of YouTube		Do not check	Note: this feature only blocks access to the YouTube app on the iOS device. The user may be able to browse to the YouTube site via the Safari browser.	GMC-11-13		

Policy Rule	Setting		Comments	Good iOS Hardening Guide Reference #	STIG ID #	VMS #
	Required	Optional				
Allow use of iTunes Music Store	Do not check  Check		Do not check for the Production Policy Set. Check for the Provisioning / SW Update Policy Set.	GMC-11-14	WIR-MOS-iOS-019	V0025012
Allow installing apps	Do not check  Check		Do not check for the Production Policy Set. Check for the Provisioning / SW Update Policy Set.	GMC-11-15	WIR-MOS-iOS-020	V0025013
Allow use of camera		Do not check		GMC-11-16	WIR-MOS-iOS-021	V0025014
Allow screen capture	Do not check		Disables screen capture but not cut & paste.	GMC-11-17	WIR-MOS-iOS-022	V0025015
Allow Game Center	Do not check		Note: This configuration setting is a future capability.	TBD	TBD	TBD
<b>WiFi Tab (No recommended or required settings)</b>						
<b>VPN Tab (No recommended or required settings)</b>						
<b>Web Clips Tab (No recommended or required settings)</b>						

This page is intentionally left blank.



**Table 2. iOS 4 Device User Based Enforcement Settings**

Policy Rule	Setting		Comments	Good Hardening Guide Reference #	STIG ID #	VMS #
	Required	Optional				
Bluetooth Radio	Off				WIR-iOS-001	V0025019
Wi-Fi Radio	Off / On		Set to off if service use is not approved. If service is approved, set to off whenever service is not being used.		WIR-iOS-002	V0025020
Wi-Fi – Ask to Join Networks	On				WIR-iOS-005	V0025092
Download iOS update via iTunes	Do not accept		Do not accept prompts to download iOS updates when device is connected to a personal computer (PC) with iTunes. Software updates will be managed by the system administrator.		WIR-iOS-003	V0025021
Location Services	Off/On		Location services should only be enabled if approved by the DAA or site IT Configuration Control Board (CCB), and only for apps specifically approved for location services.		WIR-iOS-004	V0025051
Safari – AutoFill	Off				WIR-iOS-006	V0025093
Safari – Fraud Warning		On				
Safari – JavaScript		Off	Caution should be used if this feature is enabled.			
Safari – Block Pop-ups		On	Caution should be used if this feature is disabled.			
Safari – Accept Cookies		Never or From visited				

This page is intentionally left blank.

**Table 3. List of Core iOS 4 Applications**

<b>iOS 4.1 Core Applications (iPhone)</b>	<b>OS 3.2 Core Applications (iPad)</b>	<b>iOS 4.1 Core Applications (iPod Touch)</b>
<ul style="list-style-type: none"> <li>-Phone</li> <li>-Mail</li> <li>-Safari</li> <li>-iPod</li> <li>-Messages</li> <li>-Calendar</li> <li>-Photos</li> <li>-Camera</li> <li>-YouTube (disabled by policy, icon may not be available)</li> <li>-Stocks</li> <li>-Maps</li> <li>-Weather</li> <li>-Voice Memos</li> <li>-Notes</li> <li>-Clock</li> <li>-Calculator</li> <li>-Settings</li> <li>-iTunes (disabled by policy, icon may not be available)</li> <li>-App Store (disabled by policy, icon may not be available)</li> <li>-Compass</li> <li>-Contacts</li> <li>-Nike + iPod</li> <li>-Game Center (disabled by policy, icon may not be available (future capability))</li> </ul> <p>Additional DoD Approved Apps</p> <ul style="list-style-type: none"> <li>-Good For Enterprise</li> </ul>	<ul style="list-style-type: none"> <li>-Safari</li> <li>-Mail</li> <li>-Photos</li> <li>-iPod</li> <li>-Calendar</li> <li>-Contacts</li> <li>-Notes</li> <li>-Maps</li> <li>-Videos</li> <li>-YouTube (disabled by policy, icon may not be available)</li> <li>-iTunes (disabled by policy, icon may not be available)</li> <li>-App Store (disabled by policy, icon may not be available)</li> <li>-Settings</li> </ul> <p>Additional DoD Approved Apps</p> <ul style="list-style-type: none"> <li>-Good For Enterprise</li> </ul>	<ul style="list-style-type: none"> <li>-Music</li> <li>-Videos</li> <li>-FaceTime</li> <li>-Camera</li> <li>-Photos</li> <li>-Game Center (disabled by policy, icon may not be available (future capability))</li> <li>-Mail</li> <li>-Safari</li> <li>-Calendar</li> <li>-YouTube (disabled by policy, icon may not be available)</li> <li>-Stocks</li> <li>-Maps</li> <li>-Weather</li> <li>-Notes</li> <li>-Clock</li> <li>-Calculator</li> <li>-Voice Memos</li> <li>-iTunes (disabled by policy, icon may not be available)</li> <li>-App Store (disabled by policy, icon may not be available)</li> <li>-Settings</li> <li>-Contacts</li> <li>-Nike + iPod</li> <li>-iBooks</li> </ul> <p>Additional DoD Approved Apps</p> <ul style="list-style-type: none"> <li>-Good For Enterprise</li> </ul>









This page is intentionally left blank.

## Tabular PC Pilot







## Tabular PC Pilot

## View All Site Content

## Admin Links

-  Create a post
-  Manage posts
-  Manage comments
-  Add content
-  Edit post
-  Delete post
-  Launch blog
-  Program to post

## Categories

-  Instructions
-  Technology
-  End users
-  Cascadia
-  Help Tech Support Request
-  Add new category








## RSS Feed

## Tabular PC Pilot

Welcome to the Tabular PC Pilot Web site. Use this site to capture, air concerns and requirements as well as post instructions, user surveys, ideas and feedback. Please feel free to create post and add comments. Thank you for your help. 01/2011. Again thanks for your participation.








2/22/2011

## Pilot/Experiment Clarification

2/11/2011

## Full access to Excel, Powerpoint, Word with the Ipad








      

2/3/2011

## Apps?

## Configuration Issues



      

2/1/2011







## iPad Initial Registration and Sync

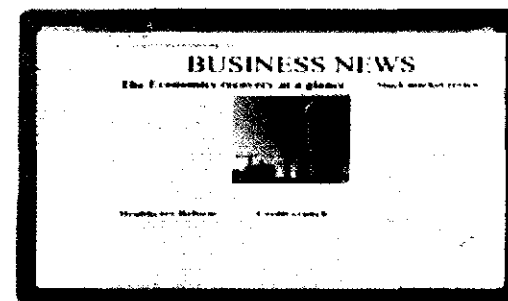
## Demo Instructions

## Pilot Help Request

## Image Web Part



## iPad Discussion Board


3/1/11

There are no comments yet. With a few more iPad Discussion Board discussions on board. To create a new comment, click "Add new discussion" below.

 Add new discussion

## DOI iPad Configuration Requirement Docs


7/26/2011


 DOI iPad Profile

 Add new document

## DOI Recommended iPad Profiles

7/26/2011

 ProfileConfig iOS6

 DOI Recommended

 Add new document

Tabular PC Pilot > Posts > Pilot/Experiment Clarification

2/22/2011

## Pilot/Experiment Clarification

[Edit](#)

I think it is very important for everyone to understand that **NO** tablet PC has been selected for addition to the BLM enterprise. This pilot/experiment is **ONLY** to test the feasibility of using this device....period. The pilot is very small because it makes no sense to procure large numbers of devices that may be found unsuitable for the BLM environment, this is why we are denying additional users to the pilot. We are going to gather and document all the pros and cons in the areas of user functionality, security, cost benefits analysis, and technical (deployment, O&M, Support) requirements.

Again, no decisions have been made nor has any edict or recommendation has been issued that would suggest a specific tablet pc (in this case iPad) is to be added. Our direction has been very clear, "conduct a **small** pilot/experiment with the iPad to determine if it is feasible device to use at BLM."

Comments: 1 (View | How do I add a comment? | Edit | How do I manage my email subscriptions? | One comment (1))

## Comments

### Pilot Roles & Responsibilities

[Edit](#)

1. W0590 (Security) is evaluating the security needs associated with iPad.
2. NOC is addressing the technical/engineering components and operational procedures.

Procedures on set-up and access of Juniper client  
 Procedures on set-up and access to Lotus Notes (email, calendars, etc)  
 How to get internal websites working via Safari  
 Use of Microsoft Office documents (Word, Excel, PowerPoint)  
 Accessing SharePoint information  
 Viewing PDFs

3. W0570 is addressing acquisitions and policy concerns if the pilot is converted to a project at the end of the pilot period.

Lewis, 2Kermit W. at 2/22/2011 11:44 AM

## Add Comment

**Title**

**Body \***



Tabular PC Pilot > Posts > Full access to Excel, Powerpoint, Word with the Ipad

2/11/2011

## Full access to Excel, Powerpoint, Word with the Ipad

Edit

Box.net app (free), it will allow word, excel, powerpoints, and pdf. It can be downloaded from iTunes, (<http://itunes.apple.com/in/app/box-net/id290853822?mt=8#>), it is really good.

Extended by: [1] Kelly Lewis, [2] Kerry W [3] Category: Help/Tech Support Request [4] Permalink [5] Email this Post [6] Comments [1]

### Comments

#### Cloud document servers - and more for Office

Edit

Are we authorized to put BLM government documents on Box.net's cloud?

Consider Citrix Receiver as another good Office Exchange service provider.

Has anyone used Office2 HD for creating/reading Office documents on the iPad - not in the Cloud. It costs about \$6 dollars. It is made for the iPhone so the screen is small.

Office to go by DataViz (\$14) also allows creation of Word, Excel, and Power PPoint docs on the iPad locally. Anyone used it?

Rawnscorett, David L [1] [2] [3] [4] [5] [6] [7] [8] [9] [10]

### Add Comment

Title

Body \*

2/3/2011

Apps?

Posted 11/20/2014 by Lewis "Zorry" W. [1] [Comment](#) [Post a Comment](#) [Feedback](#) [Email the Post](#) | [Comments \(5\)](#)

There are no comments yet for this post.

**Body \***

[illegible]



Tabular PC Pilot > Posts > Configuration Issues

2/3/2011

## Configuration Issues

[Edit](#)

Please list any installation concerns or experiences. For example, Georgia contacted us yesterday with the following information which is great. We want to know about all your concerns so we can look for ways to mitigate.

I've contacted Laura Nelson at the NOC to turn whatever feature on that the Lotus Notes servers need to serve IMAP clients. Currently it's not enabled. I've contacted Laura Nelson at the NOC, and she says she needs to get approval from Security to turn it on, hopefully you and Kerry Lewis can have some say in the matter. (Our server has it turned on due to an exception we needed to get our Pipeline Monitoring Office working. However, since the rest of the servers don't, Brandon Medrano cannot configure the mail client on Peter Ditton's iPad in Idaho.)

Respectfully,

Georgia

Published at 2:00 PM by Kerry Lewis | Category: Technology | Permalink | Edit this Post | Comments (1)

## Comments

**Turn on**

[Edit](#)

Georgia,

We are looking at and I think we have a solution to allow us to turn on the e-mail capability allowing access to Lotus Notes from the iPad. No date of when this will happen but it will be soon. More to come...

Don

Ravenbrook, Donald L. at 2/3/2011 2:05 PM

## Add Comment

**Title**

**Body \***

Tabular PC Pilot > Posts > iPad Initial Registration and Sync

2/1/2011

## iPad Initial Registration and Sync

[Edit](#)

Once the iPad is unboxed, it has to be plugged into iTunes to be registered.

Once you plug the iPad into the computer, the iPad registration comes up. Here, you have to log in or create an Apple ID.

After you log in with your iTunes Account, the fields are pre-populated with information and you just have to hit submit.

Next you choose a name for the iPad and the automatic sync settings. We chose to sync apps automatically but not to sync music automatically.

Updating to 4.2

Directly after registration and the initial sync, we had to update the iPads to 4.2.

[View iPad Initial Registration, Sync, and Update to 4.2](#) [Permalink](#) [Print](#) [Email this Post](#) [Comments \(1\)](#)

## Comments

### iPOD Required

[Edit](#)

Out of the box, the iPad doesn't have any means of connecting directly to a computer. If you happen to have and iPod (and an iTunes account, as I do), then you can connect the iPad to the computer via USB and the iPad will then recognize your iTunes account and come up.

Herbert S. S. | 2/2/2011 11:05 AM

## Add Comment

Title

Body \*

## Demo Instructions

### Demo:

#### 1.) Test VPN Connection

- Select the “**Junos Pulse**” app. Once loaded, click on **Connect**, a prompt will display: press **Accept**. You will now be presented with the “Department of the Interior, Welcome to Remote Access” screen. Scroll down and select the link under **Bureau of Land Management**. The next screen that appears is the Remote Access landing page. Scroll over to the right hand side of the screen and enter your username and password. In the username field, enter the same username you use to login to your machines at work, followed by **@.gov**, eg. **asamuels@blm.gov**, and also the same password you use to login to your machine. After you have finished entering your username and password press **Connect**. Once you are connected, the screen will display a **Disconnect** button, and your username, time connected, and VPN on will be displayed on the bottom of the screen.[b1]

#### 2.) Check email

- Select the “**Safari**” app. Click on the address bar and type in “**web.blm.gov**,” and press **Go**. Once the page has finished loading, click on **Notes Email**. A prompt will display: press **Continue**. You are now presented with the **Lotus Notes web mail** access page, enter your username and password. In the username field, enter the same username you use to login to your machines at work, and also the same password you use to login to your machine. After you have finished entering your username and password press **Connect**. A prompt will display: press **Continue**. You will now be presented with a screen titled **Server Login**. Enter your username and password in the same format as mentioned in the previous step, then press **Login**. Once the page has finished loading, you are now presented with your email.

#### 3.) Test access to internal sites

- In the “**Safari**” app select the icon that resembles an open book. Click on the various BLM links.

#### Existing Capabilities:

- View email, unable to reply and respond to emails, access to files, editing of files, access to key applications

#### Next Steps:

- Install an application to access the files on your BLM computer. Also, install a office suit app to edit Word, PowerPoint, and Excel documents.

Proctor, Don | 12:01 PM by Lewis, Jeremy | 12:01 PM | Permalink | Email This Post | Comments (1)

## Comments

### VPN Clarification

Edit

Using Junos Pulse for the first time requires configuration.

When you first download and then activate Junos please follow the following instructions:

When JUNOS asks for a username put in any string that identifies this VPN session: For example BLM Connection.

For the URL you need to provide the BLM VPN site URL:

<https://access.doi.gov/blm>

It will then think for a minute and finally bring up the BLM site. Scroll to the bottom right and then enter your username and password as described above in "test VPN Connection".

That's it !!!

I tested this using the ATT 3G connection and it worked.

Please call me at 303-236-2314 if you have questions.

Don

Ray-Hackett, Don | 12:01 PM by Lewis, Jeremy | 12:01 PM

## Add Comment

Title

Body \*



Tabular PC Pilot > Posts > Pilot Help Request

2/1/2011

## Pilot Help Request

[Edit](#)

Please list any technical or help request to this post.

Created: 2/1/2011 1:11 PM by Lewis, 2Kerry W | Category: Help/Tech Support Request | Low | Permanent | Email this Post | Comments (1)

### Comments

#### Lotus Notes IMAP Client - Enable

[Edit](#)

I have contacted the NOC and Security regarding the following configuration change request.

I've contacted Laura Nelson at the NOC to turn whatever feature on that the Lotus Notes servers need to serve IMAP clients. Currently it's not enabled. I've contacted Laura Nelson at the NOC, and she says she needs to get approval from Security to turn it on, hopefully you and Kerry Lewis can have some say in the matter. (Our server has it turned on due to an exception we needed to get our Pipeline Monitoring Office working. However, since the rest of the servers don't, Brandon Medrano cannot configure the mail client on Peter Ditton's iPad in Idaho.)

Lewis, 2Kerry W | at 2/1/2011 1:11 PM | A

### Add Comment

**Title**

**Body \***

## Comments: VPN Clarification

 Edit Item |  Delete Item |  Manage Permissions | Alert Me

**Title**

VPN Clarification

**Body**

Using Junos Pulse for the first time requires configuration.  
When you first download and then activate Junos please follow the following instructions:

When JUNOS asks for a username put in any string that identifies this VPN session: For example BLM Connection.  
For the URL you need to provide the BLM VPN site URL:

<https://access.doi.gov/blm>

It will then think for a minute and finally bring up the BLM site. Scroll to the bottom right and then enter your username and password as described above in "test VPN Connection".

That's it !!!

I tested this using the ATT 3G connection and it worked.

Please call me at 303-236-2314 if you have questions.

Don

Created at 2/22/2011 2:47 PM by Ravenscroft, Donald L

Last modified at 2/22/2011 2:47 PM by Ravenscroft, Donald L



[Tabular PC Pilot](#) > [Comments](#) > [iPOD Required](#)

## Comments: iPOD Required

 [Edit Item](#) |  [Delete Item](#) |  [Manage Permissions](#) | [Alert Me](#)

### Title

iPOD Required

### Body

Out of the box, the iPad doesn't have any means of connecting directly to a computer. If you happen to have an iPod (and an iTunes account, as I do), then you can connect the iPad to the computer via USB and the iPad will then recognize your iTunes account and come up.

Created at 2/22/2011 11:33 AM by Herbert, Scott S

Last modified at 2/22/2011 11:33 AM by Herbert, Scott S



Tabular PC Pilot > Comments > Pilot Roles & Responsibilities

## Comments: Pilot Roles & Responsibilities

 Edit Item |  Delete Item |  Manage Permissions | Alert Me

<b>Title</b>	Pilot Roles & Responsibilities
<b>Body</b>	<p>1. WO590 (Security) is evaluating the security needs associated with iPad.</p> <p>2. NOC is addressing the technical/engineering components and operational procedures.</p> <p>Procedures on set-up and access of Juniper client Procedures on set-up and access to Lotus Notes (email, calendars, etc) How to get internal websites working via Safari Use of Microsoft Office documents (Word, Excel, PowerPoint) Accessing SharePoint information Viewing PDFs</p> <p>3. WO570 is addressing acquisitions and policy concerns if the pilot is converted to a project at the end of the pilot period.</p>

Created at 2/22/2011 10:44 AM by Lewis, 2Kerry W

Last modified at 2/22/2011 10:44 AM by Lewis, 2Kerry W



Tabular PC Pilot > Comments > Cloud document servers - and more for Office

## Comments: Cloud document servers - and more for Office

 Edit Item |  Delete Item |  Manage Permissions | Alert Me

**Title** Cloud document servers - and more for Office

**Body** Are we authorized to put BLM government documents on Box.net's cloud?

Consider Citrix Receiver as another good Office Exchange service provider.

Has anyone used Office2 HD for creating/reading Office documents on the iPad - not in the Cloud. It costs about \$6 dollars. It is made for the iPhone so the screen is small.

Office to go by DataViz (\$14) also allows creation of Word, Excel, and Power Point docs on the iPad locally. Anyone used it?

Created at 2/21/2011 10:10 PM by Ravenscroft, Donald L  
Last modified at 2/21/2011 10:10 PM by Ravenscroft, Donald L