



**U.S. Department of Agriculture**

**Office of Inspector General**

---



# **USDA's Management and Security Over Wireless Handheld Devices**

**Audit Report 50501-01-IT  
August 2011**

---



United States Department of Agriculture  
Office of Inspector General  
Washington, D.C. 20250



DATE: August 15, 2011

AUDIT  
NUMBER: 50501-01-IT

TO: Christopher L. Smith  
Chief Information Officer  
Office of the Chief Information Officer  
ATTN: Sherry Linkins

Edward Knipling  
Administrator  
Agricultural Research Service  
ATTN: Michelle Garner

FROM: Gil H. Harden /s/  
Assistant Inspector General  
for Audit

SUBJECT: USDA's Management and Security Over Wireless Handheld Devices

The report presents the results of our audit of the management and security over wireless handheld devices. The response from the Office of the Chief Information Officer, which incorporates Agricultural Research Service's position, is included in its entirety in an exhibit in this report. We accept management decision for Recommendations 1 through 5, all of the recommendations in the subject audit.

We appreciate the courtesies and cooperation extended to us by members of your staff during our audit fieldwork and subsequent discussions.

## **Table of Contents**

<b>Executive Summary .....</b>	<b>1</b>
<b>Background &amp; Objectives .....</b>	<b>3</b>
<b>Background .....</b>	<b>3</b>
<b>Objectives .....</b>	<b>4</b>
<b>Section 1: Security of Wireless Handheld Devices.....</b>	<b>5</b>
<b>Finding 1: USDA Needs to Secure its Wireless Handheld Devices.....</b>	<b>5</b>
<b>Recommendation 1 .....</b>	<b>7</b>
<b>Recommendation 2 .....</b>	<b>8</b>
<b>Finding 2: USDA Needs to Better Coordinate How its TMACOs Manage     Their Agencies' Handheld Wireless Devices .....</b>	<b>8</b>
<b>Recommendation 3 .....</b>	<b>10</b>
<b>Recommendation 4 .....</b>	<b>11</b>
<b>Recommendation 5 .....</b>	<b>11</b>
<b>Scope and Methodology.....</b>	<b>12</b>
<b>Abbreviations .....</b>	<b>14</b>
<b>Exhibit A: Testing Locations .....</b>	<b>15</b>
<b>Agency's Response.....</b>	<b>16</b>

# USDA's Management and Security Over Wireless Handheld

---

## Executive Summary

Like other Federal departments, the Department of Agriculture (USDA) increasingly relies on smartphones and other handheld wireless devices to conduct its day-to-day business. These devices are small, inexpensive, and powerful, but their portability poses new security risks for Federal agencies. Since smartphones can be easily lost or stolen, misplaced devices could be used to access, and potentially abuse, private or classified information. Given concerns about the security of USDA's smartphones and other wireless handheld devices, the Office of Inspector General (OIG) initiated this audit to evaluate USDA's management and implementation of security measures over the use of mobile handheld device technology.

Of approximately 10,000 wireless handheld devices USDA uses, we selected 277 devices at the Agricultural Research Service (ARS), the Animal and Plant Health Inspection Service, the Food and Nutrition Service, the Forest Service, the National Agricultural Statistics Service, and the Office of the Chief Information Officer (OCIO).<sup>1</sup> We found that these 277 devices were not adequately secured, as defined by guidance issued by the National Institute of Standards and Technology (NIST).<sup>2</sup> For example, we found wireless handheld devices that were not password-protected, that had no anti-virus software installed, and that were not configured to encrypt removable media, among other deficiencies.<sup>3</sup> We also found that all 22 of the Department's Blackberry servers were not secured in accordance with Departmental guidance, and thus allowed users to disable their passwords or bypass the Department's internet content filters.<sup>4</sup>

Ultimately, these problems occurred because USDA chose to deploy wireless handheld devices using a decentralized approach, but did not provide its agencies with clear guidance on how they were to configure their devices and servers. The Departmental website for policies and procedures listed ten documents pertaining to wireless handheld devices, but eight documents were expired and another had been superseded. Moreover, none of these documents provided NIST-compliant security configurations for the various types of devices deployed throughout the Department.

In short, OIG found that USDA allowed these devices to proliferate throughout its agencies without establishing the guidance necessary to ensure that all agencies secured the information employees would access with these devices. Without a more centralized approach for configuring and securing these devices, USDA's data are at risk of theft, inadvertent disclosure, or manipulation.

---

<sup>1</sup> In order to select these 277 phones, we first selected 40 sites where there were particularly high concentrations of wireless devices. When we visited, we reviewed the phones that were present.

<sup>2</sup> NIST Special Publication 800-124, *Guidelines on Cell Phone and Personal Digital Assistant (PDA) Security*, October 2008.

<sup>3</sup> Removable media refers to storage media which are designed to be removed from the device without powering it off. Such media are small and easily lost or stolen if removed from the device.

<sup>4</sup> OCIO, *Baseline Configuration Standard, BlackBerry Enterprise Server Security Guide*, Revision: 1.1, dated October 24, 2007.

USDA does require its agencies to establish a telecommunications management program charged with responsibilities such as inventorying communications devices and reviewing telecommunications services and equipment to ensure they are supported by documented business need. The program is also responsible for maintaining cost-benefit analyses and all other documentation pertinent to the agency's decision for implementing telecommunications services and equipment and ensuring the most cost-effective solution for program delivery and agency compliance with USDA standards. The positions that perform these functions are known as Telecommunications Mission Area Control Officers (TMACO).

We found, however, that the agencies did not emphasize the responsibilities corresponding to these positions, and did not adequately train their TMACOs. These problems occurred because the Department did not provide adequate policies and procedures that included detailed roles and responsibilities for the TMACO position. Because there was not adequate guidance, TMACOs working for several agencies did not take steps to realize rate savings in how their agencies used handheld wireless devices, inventory their devices, or instruct their agencies' employees in how to properly use the devices.

The Department took action during the audit and issued policies that adequately addressed our concerns regarding the management of wireless devices and the roles and responsibilities of the TMACOs. Based on our review of the revised policies, we have modified our recommendations accordingly.

OIG concluded that USDA needs to take steps to secure the approximately 10,000 handheld wireless devices its employees currently use to accomplish their day-to-day business.

## **Recommendation Summary**

In this report, we have issued five recommendations, four to OCIO and one to ARS to strengthen management controls. We recommended that OCIO develop NIST-compliant configuration guides for all approved wireless handheld device and server types and monitor agencies for compliance; work with telecommunication vendors to develop and implement an electronic billing process; and develop a centralized Departmental system to capture all pertinent data for all handheld devices, such as user, phone number, make, model, device operating system, and current software level. We also made a specific recommendation to ARS to centralize its acquisitions and security over its wireless handheld devices.

## **Agency Response**

OCIO generally concurred with the recommendations and ARS concurred with the recommendation specific to the agency. OCIO incorporated ARS' position into one response. We have included the response in its entirety at the end of this report.

## **OIG Position**

We accept management decision for all 5 recommendations presented in this report.

## Background & Objectives

---

### Background

Cell phones and personal digital assistants have become indispensable tools for today's highly mobile workforce. Small and relatively inexpensive, these devices can be used not only for voice calls, simple text messages, and personal information management (e.g., phonebook, calendar, and notepad), but also for many functions performed at a personal computer, including sending and receiving email, browsing the internet, storing and modifying documents, delivering presentations, and remotely accessing data. While these devices provide productivity benefits, they also pose new security risks. Because of their small size and use outside the office, handheld devices are easier to misplace or have stolen than a notebook computer. If one of these devices is compromised, it is possible to gain access to the information stored on the device or the information the device is capable of accessing remotely.

USDA has adopted a decentralized approach to deploying wireless handheld devices—each agency is allowed to purchase devices to meet its own business needs. We found approximately 10,000 wireless handheld devices within the Department, including almost every brand and type available, though most were Blackberry smartphones. Each agency followed its own procedures for deploying the devices and implemented various levels of security.

Each agency also designates a Telecommunications Mission Area Control Officer (TMACO) who serves as the USDA agency or mission area representative on telecommunications matters, and approves orders for all telecommunications circuits, services, and equipment. The TMACO is the responsible source of technical expertise with regard to all telecommunications issues, specializing in the development, implementation, and maintenance of efficient, cost-effective telecommunications solutions.

Departmental Regulation (DR) 3300-001, Appendix B and C, *Telecommunication and Internet Services and Use*, dated March 23, 1999, requires agency and staff office managers to (1) establish internal procedures to determine the risk of, and vulnerability to, telecommunication fraud, waste, and abuse on their networks; (2) implement cost-effective actions to minimize their exposure to telecommunication fraud, waste, and abuse; (3) educate employees on telephone fraud, waste, and abuse; and (4) mitigate risks of telecommunication fraud, waste, and abuse to their systems and networks.

DR 3505-002, Appendix C, *Wireless Networking Security Policy*, dated August 11, 2009, requires agencies to ensure that all wireless network devices are configured in accordance with applicable Federal Information Processing Standards and NIST Special Publications (SP) standards.

NIST outlines many guidelines and requirements for agencies to follow as they deploy wireless equipment to their employees. NIST security practices require:

- the identification of an organization's information system assets and the development, documentation, and implementation of policies, procedures, and guidelines.

- that products of this type (smartphones and other wireless handheld devices) be checked for compliance with organizational encryption policies.
- interfaces and unneeded features be turned off until they are needed.
- devices be centrally managed to simplify the configuration control and management processes needed to ensure compliance with the organization's mobile device security policy. Agencies should be able to remotely erase, disable, or lock a device in the event it is lost or stolen.

## **Objectives**

The objective of this audit was to evaluate the management and implementation of security measures over the use of mobile handheld device technology within the Department.

## Section 1: Security of Wireless Handheld Devices

---

### Finding 1: USDA Needs to Secure its Wireless Handheld Devices

Of USDA's approximately 10,000 wireless handheld devices, we found that all 277 of those selected and tested were not adequately secured according to NIST standards.<sup>5</sup> Ultimately, these devices were not secured because USDA allowed its agencies to deploy them using a decentralized approach—essentially, permitting the agencies to purchase and use the devices they felt they needed—but did not provide the agencies with clear guidance on how to configure and use their devices securely. Unless the Department and its agencies take adequate steps to secure these devices, sensitive USDA data are at risk of theft, inadvertent disclosure, or manipulation.

NIST requires that organizations centrally manage their devices to simplify the configuration, control, and management processes needed to ensure compliance with the organization's mobile device security policy. NIST also requires that organizations inventory wireless handheld devices, conduct assessments of the risks to their devices, encrypt data on the device, install anti-virus software on the devices, use strong passwords to protect the devices, and back up any data stored on the devices.<sup>6</sup> According to the Office of Management and Budget (OMB), Federal organizations are required to comply with NIST guidance.<sup>7</sup>

We found, however, that all 277 devices we tested in 40 locations did not meet NIST standards.<sup>8</sup> Among the many deficiencies we found, 168 of these devices did not have adequate passwords, or had no passwords at all; 259 devices had no anti-virus software installed; and 139 were not configured to encrypt removable media.<sup>9</sup> If these devices were lost or stolen, potentially sensitive Government information would be easily accessible.

We also found systemic security problems with all 22 Blackberry servers the Department uses to control the approximately 10,000 devices. USDA issued the *Blackberry Enterprise Server Security Guide*, which recommended 228 settings that should be put in place on a Blackberry server to enhance security and make it more difficult for sensitive data to be compromised in the event the device is lost or stolen. However, we found that nearly 90 percent of the server settings deployed were not set in accordance with the Department's security guide. None of the deployed servers were entirely compliant with the security guide, nor did we find waivers for any noncompliant settings.

These systemic problems meant that USDA employees were able to use their devices for purposes that could compromise the security of the devices. For example, we found that five

---

<sup>5</sup> NIST SP 800-124, *Guidelines on Cell Phone and PDA Security*, dated October 2008; and OCIO, *Baseline Configuration Standard, BlackBerry Enterprise Server Security Guide*, Revision: 1.1, dated October 24, 2007.

<sup>6</sup> Ibid.

<sup>7</sup> OMB A-130, *Management of Federal Information Systems*, dated November 11, 2000.

<sup>8</sup> See Exhibit A for listing of test locations.

<sup>9</sup> Removable media refers to storage media which are designed to be removed from the device without powering it off. Such media are small and easily lost or stolen if removed from the device.

users were using a university system for their Government email, which allows potentially sensitive Government email to reside on non-Government servers. Other users were receiving non-Government email on their devices, which could allow potentially harmful and malicious software to be inadvertently loaded onto Government devices. Some users were browsing prohibited internet sites, including a gentlemen’s club site, a fantasy sports site, and a social media site.

Ultimately, these problems occurred because USDA chose to deploy these wireless handheld devices in its various agencies using a decentralized approach—agencies were allowed to purchase, configure, and use whatever smartphones or other devices they decided would be most conducive to their work—but did not provide the agencies with clear guidance on how to adequately and securely configure these devices. NIST guidelines require that organizations centrally manage their devices, since central management can provide significant security benefits.<sup>10</sup> For example, centrally managed phones could be inventoried, remotely “wiped” if stolen or lost, and have new patches installed and secure settings deployed when threats change.<sup>11</sup> Without a centrally managed solution, USDA is experiencing great discrepancies in how its agencies deploy handheld wireless devices. We found, for instance, that one agency deployed a version of iPhone with no security settings enabled.

Additionally, OIG maintains that USDA needs a more centralized approach to its wireless handheld devices, if only so that it can accurately inventory the devices it deploys. When we began this audit, the Department was unable to provide a listing of all wireless handheld devices it deployed, and referred us to the agencies, not all of whom were able to provide an accurate listing. One agency took more than 2 months to provide its inventory because it had decentralized its own deployment of these devices and had not consolidated its inventory.

To meet NIST standards, OIG believes the most direct route to secure wireless handheld devices is to centrally manage them. Additionally, USDA should consolidate and improve the guidance it provides its information technology employees. In the past, USDA has provided guidance that was not clear regarding how agencies should secure their wireless handheld devices. NIST requires that Departments and agencies create policies and procedures on key aspects of security and management over wireless handheld devices.<sup>12</sup> Of the ten documents pertaining to wireless handheld devices that USDA published on its Departmental policies and procedures website, we found that nine were superseded or expired. Nevertheless, we found agencies using the superseded and the expired policies and procedures.<sup>13</sup>

Based on our review of these ten documents, USDA’s available guidance does not meet NIST requirements because it does not provide security settings for all the types of devices deployed

---

<sup>10</sup> NIST SP 800-124, *Guidelines on Cell Phone and PDA Security*, dated October 2008; and OCIO, *Baseline Configuration Standard, BlackBerry Enterprise Server Security Guide*, Revision: 1.1, dated October 24, 2007.

<sup>11</sup> Remote wiping entails sending a signal to the sensitive Government information.

<sup>12</sup> NIST SP 800-124, device which completely obliterates all data on the device. This keeps lost or stolen phones from disclosing *Guidelines on Cell Phone and PDA Security*, dated October 2008; and OCIO, *Baseline Configuration Standard, BlackBerry Enterprise Server Security Guide*, Revision: 1.1, dated October 24, 2007.

<sup>13</sup> During the course of this audit, the Office of the Chief Information Officer removed all expired and superseded Departmental guidance from the website, and the Department began drafting new operational policies for wireless handheld devices. However, security issues were not addressed in the new operational policies.

by the agencies. At present, USDA is using Blackberry Enterprise Servers, Windows Mobile, and other enterprise solutions and servers, but the Department has no security configuration guides for these applications.

Even when the Department did provide guidance, it often prescribed security settings that were less than optimal. Although encryption is an essential means of protecting data on a mobile device if it becomes lost or stolen, OCIO provided guidance that did not mention any recommended settings for data encryption either for the device or for any associated external media (such as memory cards).

Overall, we concluded that USDA needs to take steps to improve the security of its wireless handheld devices. The Department should begin by centralizing how its agencies configure and deploy their wireless handheld devices; at a minimum, the Department must provide its agencies with clear, NIST-compliant guidance on how to configure all devices they are using. Given the seriousness of the problems we have found with USDA's security over wireless handheld devices, and the fact that these problems are pervasive in so many different agencies, we are also recommending that USDA monitor its application of these enhanced security procedures.

During the course of the audit, the Department issued a detailed policy establishing the requirements for planning and managing wireless technologies, centralizing acquisition, and addressing roles and responsibilities that cover several issues noted in this report.<sup>14</sup> Therefore, we will not be making recommendations concerning those issues that were adequately covered in the policy.

## **Recommendation 1**

Develop NIST-compliant configuration guides for all approved wireless handheld device and server types. Require agencies to document reasons for any deviations.

### **Agency Response**

OCIO concurs with this recommendation. OCIO has drafted a new Departmental Regulation, *Secure Configuration Management Policy*, based on NIST guidance. This new Departmental Regulation requires the use of Federal Government issued (e.g., NIST) secure configuration guides for all information technology devices used in USDA and the formal documentation of all deviations. OCIO anticipates the publication of the new regulation by March 31, 2012.

### **OIG Position**

OIG concurs with the management decision. OCIO has taken interim action to address this recommendation. OCIO issued instructions, effective May 26, 2011, requiring all agencies to comply with the NIST configuration guidelines.

---

<sup>14</sup> Departmental Manual (DM) 3500-005, *Policies for Planning and Managing Wireless Technologies in USDA*, dated November 10, 2010.

## Recommendation 2

Develop and implement a process to monitor wireless handheld device and server configuration settings to ensure they meet NIST requirements.

### Agency Response

OCIO concurs with this recommendation and has drafted a new Departmental Manual (DM), *USDA Secure Configuration Management Procedures*; expected publication is March 31, 2012.

### OIG Position

OIG concurs with the management decision. OCIO issued instructions, effective May 26, 2011, requiring all agencies to comply with the NIST configuration guidelines.

## Finding 2: USDA Needs to Better Coordinate How its TMACOs Manage Their Agencies' Handheld Wireless Devices

Of the 26 TMACOs working for USDA, we reviewed 6 and found that none were adequately managing and controlling how employees in their agencies used their wireless handheld devices.<sup>15</sup> Not all agencies had full-time TMACOs; some agencies had not granted their TMACOs the authority necessary to carry out their duties; and other agencies had not trained their TMACOs. These problems occurred because the Department did not centralize and coordinate the work these employees were supposed to be performing. Without greater coordination of agencies' TMACOs, different USDA agencies placed different emphasis on the TMACOs' roles and responsibilities, which resulted in USDA agencies not paying the lowest possible rates for their handheld devices, not being able to provide inventories of their devices, and not instructing employees in how they should use the devices.

USDA requires agencies to establish a telecommunications management program to include agency-wide and project-level management structures and processes responsible and accountable for managing, selecting, controlling, and evaluating investments in telecommunications systems. As part of that program, the TMACO's role includes validating telecommunication services (including handheld wireless devices); reviewing telecommunications services and equipment to ensure they are supported by documented business needs; and completing proper technical analysis. In addition, they are tasked with maintaining cost-benefit analyses and all other documentation pertinent to the agency's decision for implementing telecommunications services and equipment; and ensuring the most cost-effective solution for program delivery and agency compliance with USDA standards.<sup>16</sup>

We found, however, that the TMACOs at the six agencies we reviewed did not have the resources and the authority they needed to accomplish their duties as required by Departmental regulations:

---

<sup>15</sup> The agency TMACO is designated within each mission area/agency and is empowered to control ordering and to provide oversight when ordering network services.

<sup>16</sup> DR 3300-001, *Telecommunication and Internet Services and Use*, dated March 23, 1999.

- Four did not have policies and procedures in place for their position.
- Three TMACOs’ position descriptions defined their wireless device responsibilities as “other duties as assigned.”
- One agency –ARS– had not granted the TMACO the authority and responsibility for centralized management of wireless devices.
- Two agencies’ TMACOs were not granted authority by the agency to review telecommunication acquisitions.
- Two were not the central point-of-contact for all telecommunication services within the agency.
- Six did not maintain appropriate records for telecommunication services and justifications for the products acquired.

All of the TMACOs we interviewed stated that they had not received formal training on their assigned duties and explained that they would benefit from training in their roles and responsibilities.

One of the various responsibilities assigned to TMACOs, according to Departmental regulations, is the responsibility of ensuring that the agency is not paying more than it should for telecommunication services.<sup>17</sup> Based on our review of how the six agencies were billed over 3 months, we determined that the TMACOs were not always adequately reviewing their bills. For example, we found that:

- 109 devices had overages totaling \$23,823, including one user who had over \$1,400 in overage charges for a 3-month period while another incurred \$975 in text message and minute overages during that same period.
- 491 devices had no activity (phone or data calls) during at least one billing cycle.
- 20 employees at an agency were issued more than one phone.

OIG also noticed that the agencies were receiving most of their bills on paper, which made it difficult for the TMACOs to review their entire agency’s activity on a monthly basis—one agency’s monthly bill consisted of more than 2,600 pages. In order for a TMACO to be able to reasonably review bills of this sort, the agency needs to work with the provider to receive a consolidated, electronic bill that TMACOs can use to filter and organize the data.

In contrast, one of the agencies we reviewed—the Animal and Plant Health Inspection Service—did dedicate a TMACO to managing its telecommunications. That TMACO consolidated rate plans, discontinued unused phones, and lowered the agency’s average service line costs from \$71 to \$41 per month, saving the agency more than \$1.4 million in one year. We maintain that other agencies with a properly trained TMACO could realize similar types of savings.

OIG also found that, although managing an inventory of wireless devices is one of the responsibilities that Departmental regulations assign to TMACOs,<sup>18</sup> the agencies we reviewed

---

<sup>17</sup> Ibid.

<sup>18</sup> Ibid.

found it difficult to provide inventory information. For example, for one agency to provide us this information, the agency's TMACO needed to conduct a data call of all the agency's regions—a process that took 2 months.

Even when the six agencies we reviewed were able to produce an inventory, we found that five of their inventories differed from the lists we developed from information on the Department's servers. We also observed other problems, such as blank fields for user names; missing phone numbers, device types, and operating systems; and phone number fields populated with just the area code. Four agencies did not identify device make or model for 638 of the inventoried devices, and one agency had at least 500 unknown device makes and models on its inventory. Without this critical information being readily available, agencies will find it difficult to adequately address security incidents involving these wireless handheld devices, or deploy updates to them.

OIG maintains that TMACOs can provide USDA and its agencies with an important means of managing their telecommunications usage, particularly for wireless handheld devices. At present, however, USDA agencies are not fully utilizing this resource. USDA needs to take steps to ensure that the agencies are fully and consistently using these staff positions to comply with Departmental regulations.

During the course of this audit, the Department issued a detailed policy establishing the TMACO position, including roles and responsibilities, training, and certification that covers the issues noted in this report.<sup>19</sup> Based on our review of the revised policy, we modified our recommendations.

### **Recommendation 3**

Work with telecommunication vendors to develop and implement an electronic billing process that would allow conversion to commercially available software so that TMACOs can more easily review all bills on a monthly basis. Once in electronic format both the agency and Department should develop standard queries for detecting fraud and waste.

### **Agency Response**

OCIO concurs with this recommendation. DM 3300-005, *Policies for Planning and Managing Wireless Technologies in USDA*, November 10, 2010, addresses program requirements for the financial management of wireless communications equipment and billing. There is a current wireless billing online process that was put in place in 2009. Wireless bills are scanned by the National Finance Center (NFC), placed into a repository in St. Louis and reviewed and accessed by the TMACOs. In January 2011, OCIO started developing a replacement for the current online process; which will be announced via memo to the agencies as soon as the procurement is finalized. Once awarded, the USDA Cellular program will provide a centralized

---

<sup>19</sup> DR 3300-020, *Telecommunications Mission Area Control Officer (TMACO) Roles and Responsibilities*, August 30, 2010.

Program Office which will oversee the USDA Cellular Service Plans and inventory oversight. OCIO anticipates the award of a Blanket Purchase Agreement and project completion by March 31, 2012.

### **OIG Position**

OIG concurs with the management decision.

### **Recommendation 4**

Develop a centralized Departmental system to capture all pertinent data for all handheld devices, such as user, phone number, make, model, device operating system, and current software level.

### **Agency Response**

OCIO partially agrees with this recommendation. OCIO recognizes USDA has a decentralized procurement process for handheld devices. In its response, dated June 16, 2011, OCIO stated it is developing a memorandum explaining the unification of USDA's Cellular procurement, pricing, inventory, and management under a single program office within OCIO servicing all USDA agencies and offices through the General Services Administration and service providers. OCIO plans to issue this memorandum by July 31, 2011, and anticipates the award and completion of this project by March 31, 2012.

### **OIG Position**

OIG concurs with this management decision. The contract should include the provision for consolidating the agency inventories to a Departmentwide inventory.

### **Recommendation 5**

ARS should centralize the acquisition and security over its wireless handheld devices.

### **Agency Response**

ARS concurs with this recommendation. In its response provided to OCIO, June 2, and subsequent correspondence on July 11, 2011, ARS stated that the agency plans to implement procedures to manage the acquisition of handheld devices within ARS. Such procedures would include standardizing all ARS handheld devices, a process, requiring TMACO approved for handheld purchases, and a process to ensure security policies are installed on handheld devices prior to deployment. ARS' OCIO is currently in the process of writing formal Policy and Procedures for this process, expected completion is first quarter of fiscal year 2012.

### **OIG Position**

OIG concurs with the management decision.

## Scope and Methodology

---

Our audit focused on all wireless handheld devices that USDA operated from November 1, 2009, through April 30, 2010. We defined wireless handheld devices as machines capable of sending and receiving Government email, accessing the global contacts list, downloading software applications, and browsing the internet.

From the total population of smartphones USDA operated (approximately 10,000), we selected sites with the highest concentration of smartphones for detailed field testing. Thus, we reviewed six agencies: the Agricultural Research Service, the Animal and Plant Health Inspection Service, the Food and Nutrition Service, the Forest Service, the National Agricultural Statistics Service, and the Office of the Chief Information Officer. We then visited a total of 40 sites in 30 locations where we interviewed users and physically inspected their wireless handheld devices (see Exhibit A for a list of the locations we visited).

We ascertained whether users had been advised about the acceptable uses of the device, and that the devices had been properly configured to safeguard against network intrusion, data loss, malware, and viruses. Additionally, we wanted to ensure the Department and agencies had established policies and procedures that properly implement NIST guidelines and best practices for smartphone usage and deployment.

We designed audit tests to support our audit methodology, and ultimately, our audit objective. Specifically, we:

- devised tests to inspect smartphone server configuration settings that we then deployed to the individual devices.
- inspected Department and agency policies and procedures to ensure regulatory guidance had been implemented.
- scanned all Department Blackberry Enterprise Servers for known vulnerabilities.
- analyzed the effectiveness of the TMACOs' role, including analysis of cellular phone bills for inefficiencies and evidence of abuse.
- conducted interviews with various USDA personnel to gather information pertaining to the audit.

Additionally, our team developed standardized checklists and physically tested devices to ensure they were configured according to policy and regulatory guidelines, and were being properly utilized. Our team created a non-statistical sample of device phone numbers to test at each agency location; however, the actual testing was based on user and device availability during our site visit. After identifying a smartphone user at the agency location, we interviewed the user and inspected the user's device. The responses to each checklist question were documented and subsequently compiled into a summary spreadsheet by agency.

As a basis for the audit findings, we compared the results of the audit tests against Departmental, agency, and NIST guidance. Some of the guidance used during the course of the audit included:

- NIST SP 800-53 Revision 2, Recommended Security Controls for Federal Information Systems, December 2007.
- NIST SP 800-124, Guidelines on Cell Phone and PDA Security, October 2008.
- DR 3505-002, Wireless Networking Security Policy, August 11, 2009.
- DR 3300-001, Telecommunications and Internet Services and Use, March 23, 1999.
- Departmental Manual 3550-003, Chapter 10, Part 3: Portable Electronic Devices and Wireless Technology, February 8, 2006.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards required we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

## Abbreviations

---

ARS	Agricultural Research Service
DR	Departmental Regulation
DM	Departmental Manual
GSA	General Services Administration
NFC	National Finance Center
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
PDA	Personal Digital Assistants
SP	Special Publication
TMACO	Telecommunication Mission Area Control Officer
USDA	United States Department of Agriculture

## **Exhibit A: Testing Locations**

---

The following locations were visited by OIG during the course of the audit.

- Phoenix, Arizona
- Tucson, Arizona
- Denver, Colorado
- Fort Collins, Colorado
- Dover, Delaware
- Washington, District of Columbia
- Fort Pierce, Florida
- Chicago, Illinois
- Lombard, Illinois
- Ames, Iowa
- Des Moines, Iowa
- Manhattan, Kansas
- Topeka, Kansas
- Annapolis, Maryland
- Beltsville, Maryland
- Columbia, Missouri
- Jefferson City, Missouri
- Kansas City, Missouri
- Springfield, Missouri
- Albuquerque, New Mexico
- Raleigh, North Carolina
- Research Park, North Carolina
- Corvallis, Oregon
- Eugene, Oregon
- Tangent, Oregon
- Arlington, Virginia
- Rosslyn, Virginia
- Olympia, Washington
- Pullman, Washington
- Spokane, Washington

**USDA'S**

**OFFICE OF CHIEF INFORMATION  
OFFICER AND AGRICULTURAL RESEARCH  
SERVICE**

**RESPONSE TO AUDIT REPORT**



JUN 16 2011

United States  
Department of  
Agriculture

Office of the Chief  
Information Officer

1400 Independence  
Avenue S.W.

Washington, DC  
20250

TO: Gil H. Harden  
Assistant Inspector General for Audit  
Office of Inspector General

FROM: Christopher L. Smith   
Chief Information Officer  
Office of the Chief Information Officer

SUBJECT: USDA's Management and Security Over Wireless Handheld Devices  
(Audit 50501-1-IT) DRAFT

Thank you for the opportunity to review and provide comments on the subject draft audit report.

**Finding 1: USDA Needs to Secure its Wireless Handheld Devices**

**Recommendation 1:** Develop National Institute of Standards and Technology (NIST)-compliant configuration guides for all approved wireless handheld device and server types. Require agencies to document reasons for any deviations.

**Office of the Chief Information Officer (OCIO) Response**

OCIO agrees with this recommendation. OCIO has drafted a new Departmental Regulation (DR) titled "Secure Configuration Management Policy" based on NIST guidance. This DR will supersede Departmental Manual (DM) 3520-000 Configuration Management, dated, 07/15/04, 3520-001; CM Policy & Responsibilities, dated 7/17/04; 3535-000 C2 Controlled Access Protection – General Information, dated 5/11/05; and 3535-001 USDA's C2 Level of Trust, dated 02/17/05. This new DR requires the use of Federal Government issued (e.g. NIST) secure configuration guides for all information technology devices used in USDA and formal documentation of all deviations. This regulation is currently in OCIO review.

Additionally, on May 26, 2011, the Associate Chief Information Officer (ACIO) for the Agriculture Security Operations Center (ASOC) issued a memorandum to all agency Chief Information Officers and Information Systems Security Program Managers requiring the use of NIST Security Configuration Checklists.

Estimated Completion Date: We anticipate publication of the new DR by March 31, 2012.

**Recommendation 2:** Develop and implement a process to monitor wireless handheld device and server configuration settings to ensure they meet NIST requirements.

**OCIO Response**

OCIO agrees with this recommendation. OCIO has drafted a new DM titled "USDA Secure Configuration Management Procedures." This manual is currently in OCIO review.

Estimated Completion Date: We anticipate publication of the new DM by March 31, 2012.

**Finding 2: USDA Needs to Better Coordinate How its Telecommunications Mission Area Control Officers (TMACOs) Manage Their Agencies' Handheld Wireless Devices**

**Recommendation 3:** Work with telecommunication vendors to develop and implement an electronic billing process that would allow conversion to commercially available software so that TMACOs can more easily review all bills on a monthly basis. Once in electronic format both the agency and Department should develop standard queries for detecting fraud and waste.

**OCIO Response**

OCIO agrees with this recommendation. DM3300-005, Policies for Planning and Managing Wireless Technologies in USDA, November 10, 2010, addresses program requirements for the financial management of wireless communications equipment and billing. There is a current wireless billings online process that was put in place in 2009. Wireless bills are scanned by the National Finance Center and placed into a repository in St. Louis and reviewed and accessed by the TMACO's. In January 2011, OCIO started developing a replacement for the current online process, which will be announced via memo to the agencies as soon as the procurement is finalized. Once awarded the USDA Cellular program will provide a centralized Program Office which will oversee the USDA Cellular Service Plans and the inventory oversight.

Estimated Completion Date: We anticipate award of a BPA and completion by March 31, 2012.

**Recommendation 4:** Develop a centralized Departmental system to capture all pertinent data for all handheld devices, such as user, phone number, make, model, device operating system, and current software level.

**OCIO Response**

OCIO partially agrees with this recommendation. USDA has a decentralized procurement process for handheld devices. Agencies maintain their own inventory information. OCIO is developing a memorandum to unify USDA Cellular procurement, pricing, inventory, and management under a single program office within OCIO, servicing all USDA agencies and offices and the enterprise representative to the General Services Administration and service providers. OCIO will implement a solution for TMACO's to use for inventory management for all agencies' wireless devices. OCIO will issue the memorandum by July 2011.

Estimated Completion Date: We anticipate award and completion by March 31, 2012.

**Recommendation 5:** The Agriculture Research Service (ARS) should centralize the acquisition and security over its wireless handheld devices.

**OCIO Response**

OCIO and ARS agree with this recommendation.

Due to the decentralized budgetary process within ARS, the agency plans to implement the following procedures to manage the acquisition of handheld devices within ARS:

- Standardize all ARS handheld devices that will be identified as supported in the USDA Enterprise Messaging System;
- Utilize a process that is routed through the Agency TMACO to approve handheld purchases;
- TMACO approves purchase and documents specificities in a managed database;
- Unsupported devices would be sent through the TMACO as a “waiver process” with the Department having the final approval; and
- All handheld devices will have Department security policies applied through one of two processes.

**Security**

- Once connected the Department Enterprise Messaging System (EMS) security policies are installed on hand held devices.
- Handheld devices not connected to Department EMS will be provisioned with security policies by local IT specialists before being deployed for use.

Estimated Completion Date: Pending Departmental guidance on wireless technologies will be supported in the BPOS EMS.

OCIO will continue to keep the Office of Inspector General abreast of our progress on these recommendations. If further information is needed, please contact Sherry Linkins, OCIO Audit Liaison at 202-720-9293.

cc:

Charles T. McClam, Deputy Chief Information Officer

Richard Coffee, Acting ACIO-CPPO

Christopher Lowe, ACIO-ASOC

Lennetta Elias, Program Analyst, OCFO

Owen Unangst, Director-IOA

Sherry Linkins, OCIO

Cynthia Schwind, OCIO