Office of Audits
Office of Inspector General
U.S. General Services Administration

Audit of GSA's Mobile Computing Initiatives

Report Number A130016/O/F/F13003
September 10, 2013

Office of Audits
Office of Inspector General
U.S. General Services Administration

REPORT ABSTRACT

OBJECTIVE

The objective of this audit was to determine whether the General Services Administration's (GSA) implementation of initiatives for mobile devices and mobile applications was consistent with its information technology (IT) strategic goal for access to GSA systems from Any Location, Anytime, and Any Device (A3) and the White House's Digital Government Strategy. Specifically, this audit focused on the following:

- Did the GSA Office of the Chief Information Officer (OCIO) fulfill its milestone actions related to mobile devices and mobile applications under the White House's Digital Government Strategy?
- Did the GSA Chief Information Officer's (CIO) policies and procedures for mobile computing sufficiently address security and privacy controls for mobile devices and mobile applications, include sufficient GSA user training, and include approval of mobile application terms of service?
- Were GSA's services and staff offices adhering to GSA OCIO guidance on mobile computing?

Finance & Information Technology Audit Office
1800 F Street, NW, Suite 5215
Washington DC 20405
202-273-7322

Audit of GSA's Mobile Computing Initiatives

Report Number A130016/O/F/F13003
September 10, 2013

WHAT WE FOUND

We identified the following during our audit:

Finding 1 – GSA lacks comprehensive standards for mobile application security, privacy, and development, increasing risk to deployed mobile applications.

Finding 2 – GSA OCIO guidance on mobile device acquisition does not sufficiently address risks associated with brand name specifications and could result in excessive expenditures and contractor protests to awards.

Finding 3 – GSA's mobile device assessment process was not documented, which could result in knowledge loss due to personnel disruptions.

WHAT WE RECOMMEND

Based on our audit findings we recommend the GSA CIO:

1. Develop comprehensive standards for mobile applications including:
    a. Security standards to address the following risks:
        i. Exploitation of vulnerabilities due to poor programming practices
        ii. Compromise of sensitive application data
        iii. Not completing security assessment and authorization requirements
    b. Privacy standards to include directions on creating and distributing privacy notices.
    c. Development standards to identify mobile platforms to target for publicly available applications.
2. Ensure that currently deployed mobile applications meet the updated standards.
3. Issue guidance and/or training related to tablet device acquisition to remind acquisition personnel about requirements for brand name specifications.
4. Formally document the process for reviewing mobile devices.

MANAGEMENT COMMENTS

Management agreed with our findings and recommendations. The GSA CIO's complete response is presented in **Appendix B.**

Office of Audits
Office of Inspector General
U.S. General Services Administration

DATE: September 10, 2013

TO: Casey Coleman
Chief Information Officer (I)

FROM: Donna Peterson-Jones Donna Peterson-Jones
Audit Manager, (JA-F)

SUBJECT: Audit of GSA's Mobile Computing Initiatives
A130016/O/F/F13003

This report presents the results of our audit of GSA's Mobile Computing Initiatives. Our findings and recommendations are summarized in the Report Abstract. Instructions regarding the audit resolution process can be found in the email that transmitted this report.

Your written comments to the draft report are included in Appendix B of this report.

If you have any questions regarding this report, please contact me or any member of the audit team at the following:

Donna Peterson-Jones	Audit Manager	donna.peterson@gsaig.gov	202-273-7334
Terry Williams	Auditor-In-Charge	terry.williams@gsaig.gov	202-273-7329
Dominique Lipscomb	Management Analyst	dominique.lipscomb@gsaig.gov	202-273-7322
Damian Pryor	Management Analyst	damian.pryor@gsaig.gov	202-273-7322
Steven Swantek	Auditor	steven.swantek@gsaig.gov	202-273-7322

On behalf of the audit team, I would like to thank you and your staff for your assistance during this audit.

Table of Contents

Introduction

One of the General Services Administration's (GSA) information technology (IT) strategic goals is to provide access to GSA systems from Any Location, Anytime, and Any Device (A3).[1] The A3 goal has two initiatives relating to mobile devices and mobile applications. One initiative seeks to provide the GSA workforce with secure access to GSA's IT resources and systems regardless of how, where, or when they are working. The second seeks to transform enterprise and legacy applications using modern technologies (e.g. middleware, web, and mobile computing), architecture, and frameworks to enable access from any device, anywhere, and at anytime.

Specific GSA actions associated with A3 include procuring and connecting mobile devices to GSA systems, optimizing existing web sites for mobile use, and developing mobile applications for its legacy systems. GSA has implemented a mobile device management platform to assist in controlling access to enterprise resources, such as email and virtual desktop connections. At the time of our audit, GSA had developed four mobile applications for legacy web sites that were publicly available on the Apple or Google Play mobile application stores. In addition, GSA was in the process of developing other mobile applications for internal use.

On August 2, 2011, GSA decentralized the acquisition of mobile devices. At that time, the GSA Chief Information Officer (CIO) issued an instructional letter to the Heads of Services and Staff Offices and Regional Administrators delegating responsibility for the acquisition of tablet devices to the services and staff offices.[2]

On May 23, 2012, the White House launched the Digital Government Strategy to coordinate efforts and focus on taking an information- and customer-centric approach to changing how the government works and delivers services.[3] Digital Government Strategy milestone actions include a requirement that agencies improve priority, customer-facing services for mobile use.

The objective of this audit was to determine whether GSA's implementation of initiatives for mobile devices and mobile applications was consistent with its IT strategic goal for access to GSA systems from A3 and the White House's Digital Government Strategy. Specifically, this audit focused on the following:

- Did the GSA Office of the Chief Information Officer (OCIO) fulfill its milestone actions related to mobile devices and mobile applications under the White House's Digital Government Strategy?

[1] *GSA FY12–15 Information Technology Strategic Business Plan,* http://www.gsa.gov/graphics/staffoffices/itstrategicplan2012.pdf.
[2] GSA *CIO IL-11-01, Smart Phone and Tablet Device Acquisition and Support Policy,* August 2, 2011.
[3] *Digital Government: Building a 21st Century Platform to Better Serve the American People,* http://www.whitehouse.gov/sites/default/files/omb/egov/digital-government/digital-government.html.

- Did the GSA CIO policies and procedures for mobile computing sufficiently address security and privacy controls for mobile devices and mobile applications, include sufficient GSA user training, and include approval of mobile application terms of service?
- Were GSA's services and staff offices adhering to GSA OCIO guidance on mobile computing?

See ***Appendix A*** – Purpose, Scope, and Methodology for additional details.

Results

Finding 1 – GSA lacks comprehensive standards for mobile application security, privacy, and development, increasing risk to deployed mobile applications.

GSA has released mobile applications that were not assessed for mobile security risks, lacked privacy notices, and/or inconsistently targeted mobile platforms. This resulted from GSA not comprehensively addressing security, privacy, and development risks in standards relating to mobile applications.

Standards for security of mobile applications

While GSA requires all applications to undergo GSA's security assessment and authorization process in accordance with the Federal Information Security Management Act of 2002 (FISMA[4]), none of the released mobile applications underwent required security assessments and authorizations. Developers of these mobile applications did not deem this requirement to be applicable prior to release to the Apple or Google Play mobile application stores. However, not completing these required activities reduces the assurance that security requirements for systems are being implemented correctly, operating as intended, and producing the desired outcome.

GSA developed and released four mobile applications. After the release, GSA OCIO established procedures specifying the required evaluations for mobile applications (both GSA developed and commercially developed) using the National Institute of Standards and Technologies (NIST) Special Publication (SP) 800-53 controls.[5] However, we determined that these controls did not comprehensively address mobile security risks. The risks identified in the Open Web Application Security Project (OWASP) Mobile Security Project included weak server side controls, insecure data storage, and insufficient transport layer protections.[6] Exploitation of these risks could affect the confidentiality, integrity, or availability of deployed mobile applications. In addition, our evaluation of the four GSA developed mobile applications found that none were assessed for these mobile-specific risks.

Standards for privacy of mobile applications

Privacy information that could be captured from a mobile application includes device identifications, location, camera and/or photos, Internet Protocol (IP) addresses, and contacts. A privacy notice helps ensure that the public has notice and choice about, and thus confidence in, how their personal information is handled when they use the mobile applications. Best practices identified in a Federal Trade Commission report

[4] FISMA requires agencies to develop and maintain minimum controls required to protect federal information and information systems.

[5] NIST SP 800-53, *Recommended Security Controls for Federal Information Systems and Organizations,* Rev. 3, August 2009.

[6] OWASP is a not-for-profit organization focused on improving the security of software. The OWASP Mobile Security Project is a centralized resource intended to give developers and security teams the resources they need to build and maintain secure mobile applications. See https://www.owasp.org/index.php/OWASP_Mobile_Security_Project.

recommended that mobile application developers ensure that their privacy notice is easily accessible through the app stores.[7] However, GSA has not developed privacy standards for mobile applications to ensure that publicly available applications include privacy notices. Our evaluation of GSA's mobile applications found that none had privacy notices specific to data usage captured from the use of mobile applications. The lack of privacy notices could reduce the public's confidence that GSA will appropriately use their information.

Standards for development of mobile applications

According to GSA's System Development Life Cycle Policy,[8] the GSA CIO assumes responsibility for assuring that IT is well governed in GSA, including establishing and maintaining local system development life cycle processes, practices, standards, and governance. However, GSA's development standards have not been updated to identify target platforms for mobile applications developed for the public (e.g., Android or Apple iOS). As a result, GSA's approach to targeting platforms has been inconsistent. In fact, one GSA staff office developed one mobile application only for Android, and developed another mobile application only for Apple's iOS. Since the purpose of these mobile applications is to reach the public, inconsistent targeting of platforms limits GSA's audience.

Finding 2 – GSA OCIO guidance on mobile device acquisition does not sufficiently address risks associated with brand name specifications and could result in excessive expenditures and contractor protests to awards.

We identified two acquisitions for 19 iPads and accessories totaling $14,775.34 that were made using brand name specifications. The Federal Acquisition Regulation (FAR) 11.104-11.105 prohibits the use of brand name specifications except under very limited circumstances.[9] We believe the improper specification of brand names is of particular concern in tablet device acquisitions because preferences derived from personal experiences tend to be particularly strong when it comes to mobile devices.[10] However, GSA Instructional Letter *CIO IL-11-01 Smart Phone and Tablet Device Acquisition and Support Policy* does not provide guidance related to brand name specification requirements for tablet device acquisitions. The agency's use of brand name specifications could result in excessive expenditures in tablet device acquisitions due to the lack of full and open competition and could increase the risk of contractor protests to agency contract awards.

[7] *Mobile Privacy Disclosures, Building Trust Through Transparency*, February 2013, http://www.ftc.gov/os/2013/02/130201mobileprivacyreport.pdf.

[8] GSA Order CIO 2140.3, *CIO Systems Development Life Cycle (SDLC) Policy,* September 29, 2006.

[9] For the purposes of this audit, a brand name specification is defined as a description that specifies a particular brand name, product, or product feature that is peculiar to one manufacturer. (FAR 11.105)

[10] According to Pew Research Center's Project for Excellence in Journalism, mobile device operating system loyalty is exhibited among those that have both a tablet computer and a smartphone. See http://www.journalism.org/analysis_report/device_ownership.

Finding 3 – GSA's mobile device assessment process was not documented, which could result in knowledge loss due to personnel disruptions.

According to Office of Management and Budget Circular A-123, management needs to ensure that appropriate policies, procedures, and mechanisms exist with respect to each of the agency's activities. However, the security assessment for GSA's mobile devices has not been documented. The Office of the Senior Agency Information Security Officer (OSAISO) has one staff member reviewing mobile devices for GSA employees prior to approval for access to GSA internal systems. Since the process is not documented, if GSA loses the employee, it will no longer have knowledge of the process or of the requirements.[11]

Recommendations

Based on our audit findings we recommend the GSA Chief Information Officer:

1. Develop comprehensive standards for mobile applications including:
   a. Security standards to address the following risks:
      i. Exploitation of vulnerabilities due to poor programming practices
      ii. Compromise of sensitive application data
      iii. Not completing security assessment and authorization requirements
   b. Privacy standards to include directions on creating and distributing privacy notices.
   c. Development standards to identify mobile platforms to target for publicly available applications.

2. Ensure that currently deployed mobile applications meet the updated standards.

3. Issue guidance and/or training related to tablet device acquisition to remind acquisition personnel about requirements for brand name specifications.

4. Formally document the process for reviewing mobile devices.

Management Comments

Management agreed with our findings and recommendations. The GSA CIO's complete response is presented in ***Appendix B.***

[11] During the audit the OSAISO provided a checklist of requirements including encryption and proper functioning in the GSA mobile device management platform for device approval.

Conclusion

We found that GSA is making progress in its IT strategic goal to provide enhanced mobile access to GSA systems and data. First, GSA fulfilled its milestone actions related to mobile devices and mobile applications under the White House's Digital Government Strategy by prioritizing two existing, major, customer-facing services for modernization. Second, our evaluation of the mobile device management platform identified that it enforces security controls for mobile devices in accordance with GSA requirements. Third, user training on mobile devices informs users of mobile-specific security concerns. Fourth, GSA reviews terms of service for mobile applications before approval for agency use.

However, GSA can strengthen the implementation of its mobile computing initiatives by:

(1) Developing comprehensive standards for mobile application security, privacy, and development;
(2) Ensuring that mobile applications undergo required security assessment and authorizations and meet updated standards;
(3) Providing guidance on mobile device acquisition that sufficiently addresses risks associated with brand name specifications, specifically to prevent excessive expenditures and contractor protests; and
(4) Documenting processes to ensure continuity of GSA's mobile device assessments to prevent knowledge loss in case of personnel disruptions.

We believe that making the improvements recommended in this report will better enable GSA to provide enhanced mobile access to the agency's systems and data.

Appendix A – Purpose, Scope, and Methodology

Purpose

This audit was performed to assess GSA's actions to provide enhanced mobile access to government systems and data. It was included in the Office of Inspector General's Fiscal Year (FY) 2013 Audit Plan.

Scope

The audit's scope includes results of the Office of Inspector General's evaluations of the OCIO's oversight of the implementation of the GSA's mobile computing initiatives as it relates to mobile devices and applications.

Methodology

To accomplish our objectives, we:

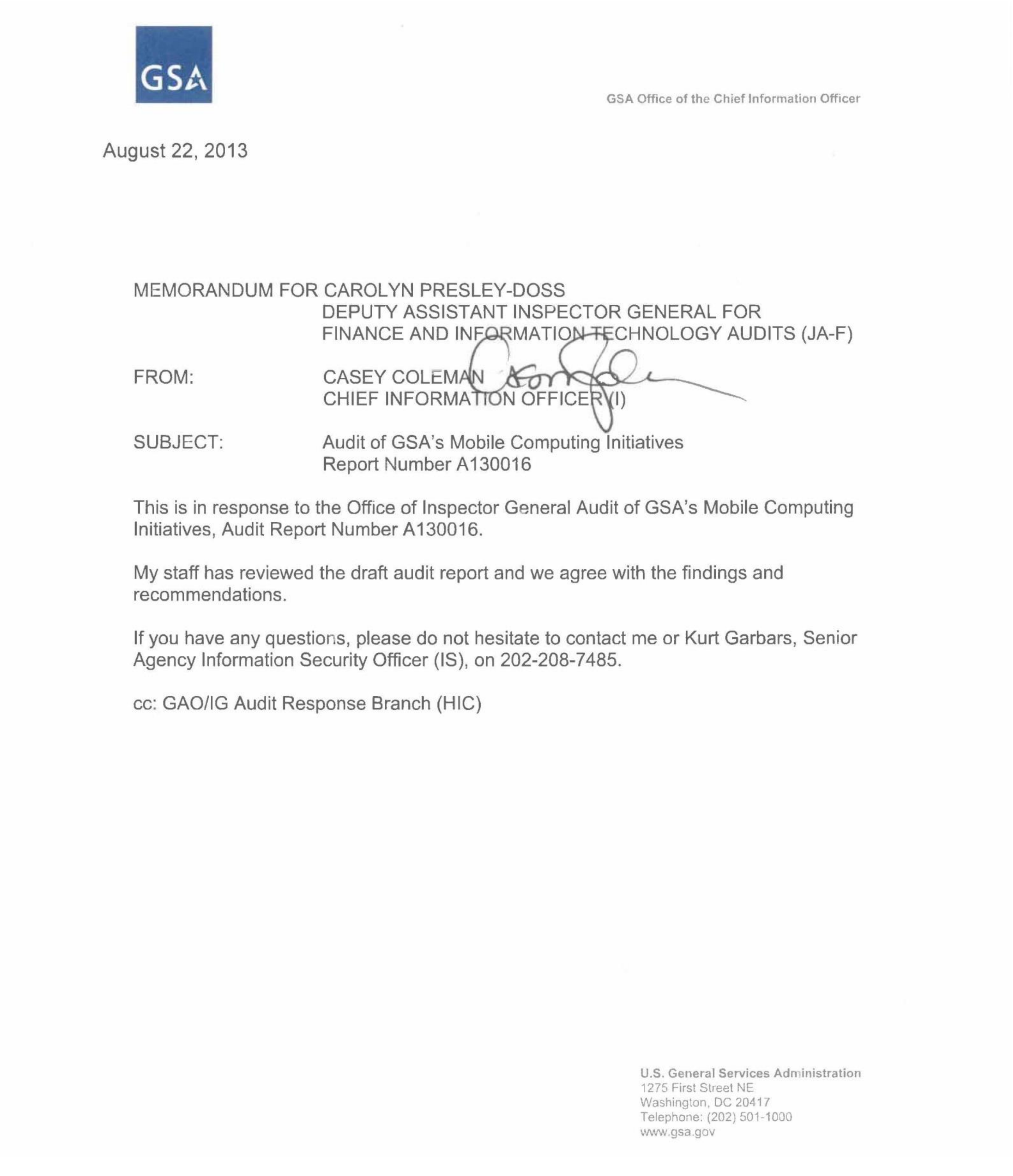
- Interviewed OCIO officials implementing mobile computing initiatives associated with its A3 strategy.
- Interviewed mobile application developers in the Federal Acquisition Service, Office of Government-Wide Policy, Office of Citizen Services and Innovative Technologies, and Office of the Chief Information Officer.
- Performed walkthroughs to verify: (1) controls to manage mobile devices in GSA's mobile device management platforms and (2) controls for security testing of mobile platforms.
- Reviewed applicable mobile device and application privacy, security, development, and acquisition regulations, policies, and guidance.
- Reviewed GSA's services and staff offices' adherence to GSA CIO guidance on mobile computing by: (a) testing deployed mobile applications for security controls, privacy controls, and adherence to development standards and (b) evaluating tablet computer purchases for compliance with procurement regulations (e.g. Trade Agreements Act, fair opportunity, and brand name purchases).

We conducted the audit between October 2012 and March 2013 in accordance with generally accepted government auditing standards. Those standards require that 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.

Internal Controls

This audit included a review of elements of GSA's mobile computing initiatives, relating to management of mobile devices, oversight of mobile application development, and limited testing of controls over acquisition of mobile tablets. The *Results* and *Recommendations* sections of this report state, in detail, the need to strengthen specific processes and controls in implementation of the GSA CIO's mobile computing initiatives.

Appendix B – Management Comments



GSA

GSA Office of the Chief Information Officer

August 22, 2013

MEMORANDUM FOR CAROLYN PRESLEY-DOSS
DEPUTY ASSISTANT INSPECTOR GENERAL FOR
FINANCE AND INFORMATION TECHNOLOGY AUDITS (JA-F)

FROM: CASEY COLEMAN
CHIEF INFORMATION OFFICER (I)

SUBJECT: Audit of GSA's Mobile Computing Initiatives
Report Number A130016

This is in response to the Office of Inspector General Audit of GSA's Mobile Computing Initiatives, Audit Report Number A130016.

My staff has reviewed the draft audit report and we agree with the findings and recommendations.

If you have any questions, please do not hesitate to contact me or Kurt Garbars, Senior Agency Information Security Officer (IS), on 202-208-7485.

cc: GAO/IG Audit Response Branch (HIC)

U.S. General Services Administration
1275 First Street NE
Washington, DC 20417
Telephone: (202) 501-1000
www.gsa.gov

Appendix C – Report Distribution

GSA Chief Information Officer (I)

Senior Agency Information Security Officer (IS)

Division Director, GAO/IG Audit Response Division (H1C)

Audit Liaison, Office of the Chief Information Officer (I)

Assistant Inspector General for Auditing (JA)

Deputy Assistant IG for Investigations (JID)

Director, Audit Planning, Policy, and Operations Staff (JAO)