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

IMPLEMENTATION REVIEW OF ACTION PLAN

Audit of GSA's Mobile Computing Initiatives Report Number A130016/O/F/F13003 September 10, 2013

Assignment Number A150044
January 13, 2015

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

DATE: January 13, 2015

TO: Sonny Hashmi
Chief Information Officer (I)

FROM: Susan P. Hall Susan P. Hall
Audit Manager, Program Audit Office (JA-R)

SUBJECT: Implementation Review of Action Plan
Audit of GSA's Mobile Computing Initiatives
Report Number A130016/O/F/F13003
September 10, 2013
Assignment Number A150044

We have completed an implementation review of the management actions taken in response to the recommendations contained in the subject audit report (see ***Appendix A***). The objective of our review was to determine whether the Office of GSA IT[1] has taken the corrective actions as outlined in the Action Plan for the *Audit of GSA's Mobile Computing Initiatives*. To accomplish our objective we:

- Examined documentation submitted by the Office of GSA IT supporting accomplishment of the action plan steps;
- Performed limited testing of the implementation of the guidance and procedures contained in these supporting documents; and
- Met and corresponded with Office of GSA IT personnel.

Our implementation review found that the Office of GSA IT addressed the audit recommendations in the action plan, dated November 5, 2013.

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

Susan P. Hall	Audit Manager	susan.hall@gsaig.gov	(202) 501-2073
Greg Kepner	Auditor-in-Charge	gregory.kepner@gsaig.gov	(202) 273-4999

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

[1] The original audit report was issued to the Office of the Chief Information Officer. This office was recently renamed the Office of GSA IT.

Background

On September 10, 2013, we issued an audit report, *Audit of GSA's Mobile Computing Initiatives,* to the Office of GSA IT. One of GSA's information technology goals was to provide access to GSA systems from any location, at any time, and on any device. This goal was supported by two initiatives relating to mobile devices and mobile applications. One initiative was to provide the GSA workforce with secure access to GSA's information technology resources and systems regardless of how, where, or when they are working. The second initiative was to transform enterprise and legacy applications using modern technologies, architecture, and frameworks to enable access from any device, anywhere, and at any time.

Specific GSA actions associated with this overall goal included procuring and connecting mobile devices to GSA systems, optimizing existing web sites for mobile use, and developing mobile applications for GSA's legacy systems. GSA 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 the initial audit, GSA developed four mobile applications for legacy web sites that were publicly available on the Apple or Google Play mobile application stores.

The original audit found:

- GSA lacks comprehensive standards for mobile application security, privacy, and development which increases risk to deployed mobile applications.
- The Office of GSA IT 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.
- GSA's mobile device assessment process was not documented, which could result in knowledge loss due to personnel disruptions.

To address the issues identified in the report, we recommended that the 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.

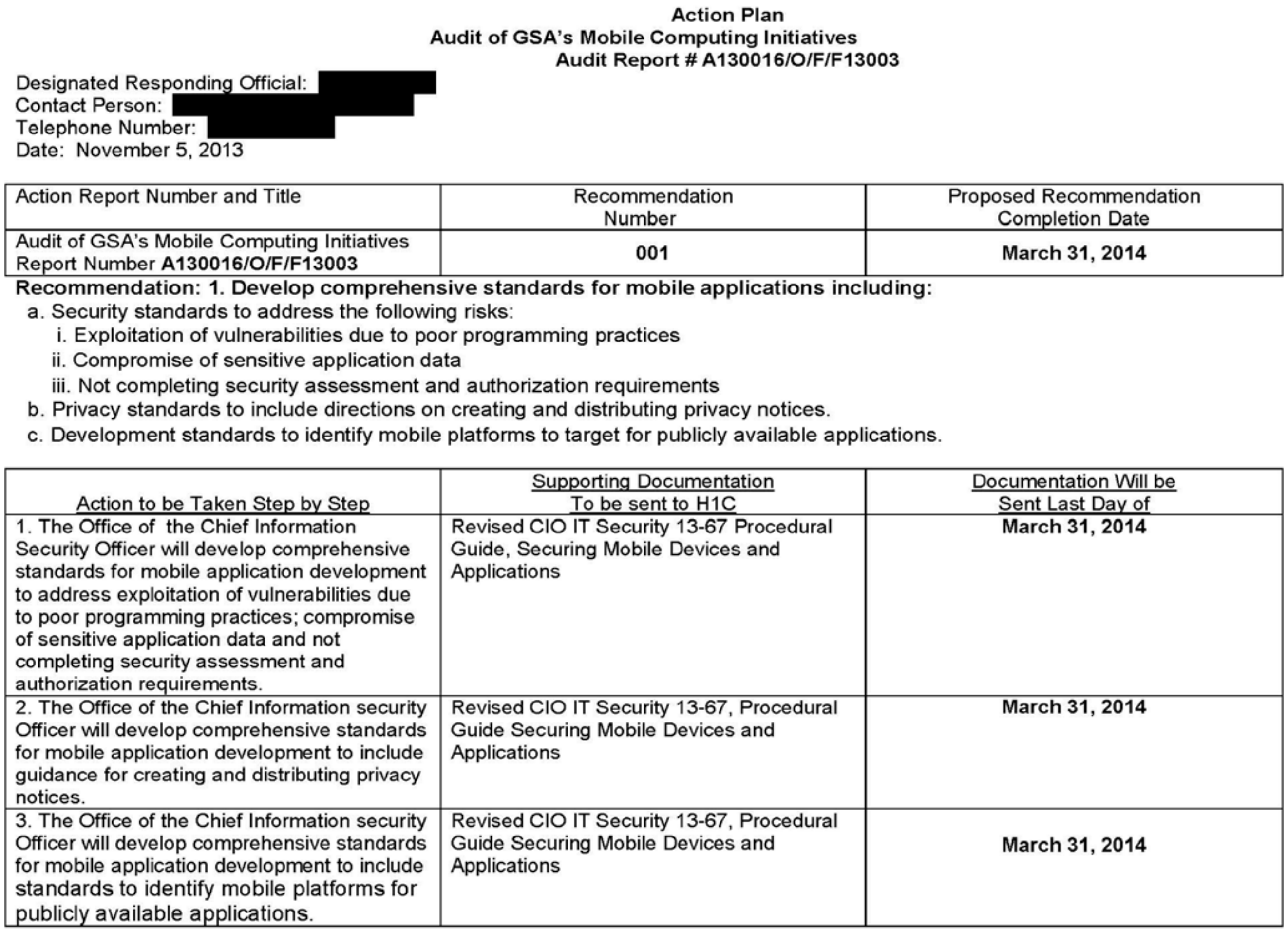
3. Issue guidance and/or training related to tablet device acquisition to remind acquisition personnel about requirements for brand name specifications.
4. Formally document the process for reviewing mobile devices.

The Chief Information Officer agreed with the report recommendations.

Results

Our implementation review found that the Office of GSA IT has taken appropriate corrective actions to address the recommendations. We determined that no further action is necessary to address our recommendations.

Appendix A – Action Plan for Report Number A130016/O/F/F13003



Action Plan
Audit of GSA's Mobile Computing Initiatives
Audit Report # A130016/O/F/F13003

Designated Responding Official: [redacted]
Contact Person: [redacted]
Telephone Number: [redacted]
Date: November 5, 2013

Action Report Number and Title	Recommendation Number	Proposed Recommendation Completion Date
Audit of GSA's Mobile Computing Initiatives Report Number **A130016/O/F/F13003**	**001**	**March 31, 2014**

Recommendation: 1. Develop comprehensive standards for mobile applications including:

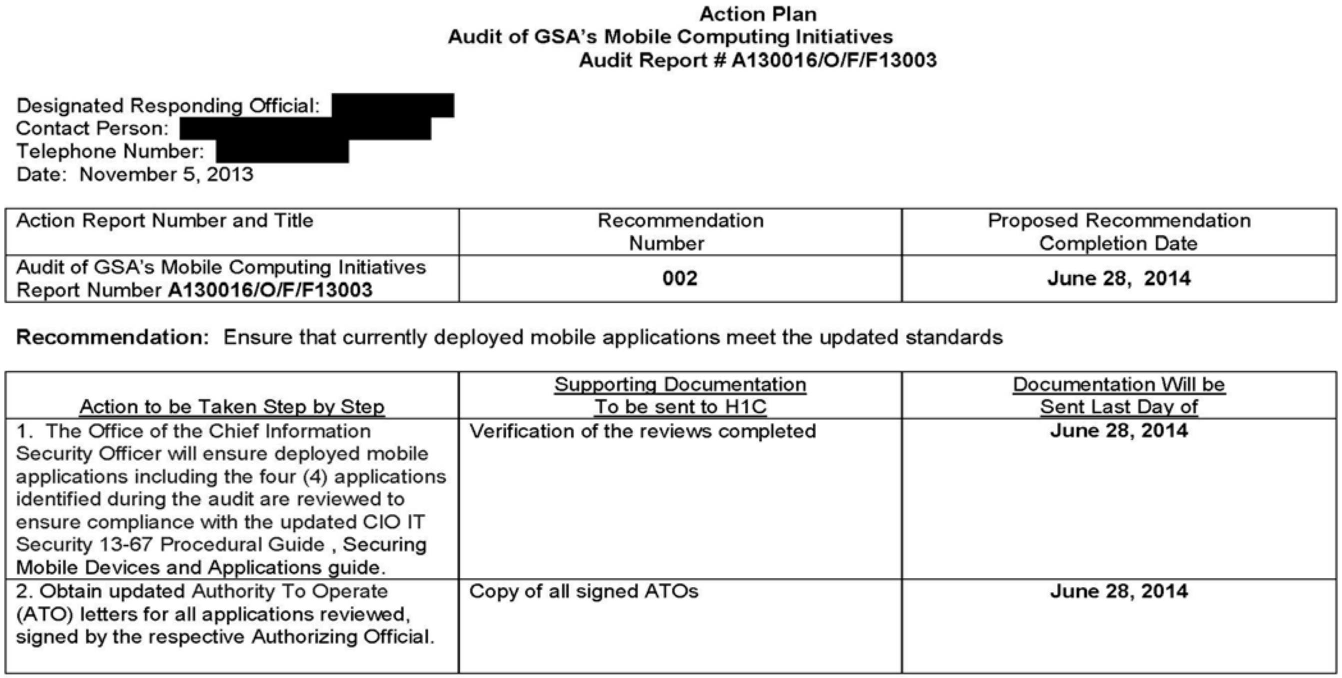
a. Security standards to address the following risks:
   i. Exploitation of vulnerabilities due to poor programming practices
   ii. Compromise of sensitive application data
   iii. Not completing security assessment and authorization requirements

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.

Action to be Taken Step by Step	Supporting Documentation To be sent to H1C	Documentation Will be Sent Last Day of
1. The Office of the Chief Information Security Officer will develop comprehensive standards for mobile application development to address exploitation of vulnerabilities due to poor programming practices; compromise of sensitive application data and not completing security assessment and authorization requirements.	Revised CIO IT Security 13-67 Procedural Guide, Securing Mobile Devices and Applications	**March 31, 2014**
2. The Office of the Chief Information security Officer will develop comprehensive standards for mobile application development to include guidance for creating and distributing privacy notices.	Revised CIO IT Security 13-67, Procedural Guide Securing Mobile Devices and Applications	**March 31, 2014**
3. The Office of the Chief Information security Officer will develop comprehensive standards for mobile application development to include standards to identify mobile platforms for publicly available applications.	Revised CIO IT Security 13-67, Procedural Guide Securing Mobile Devices and Applications	**March 31, 2014**

Appendix A – Action Plan for Report Number A130016/O/F/F13003 (cont.)



Action Plan
Audit of GSA's Mobile Computing Initiatives
Audit Report # A130016/O/F/F13003

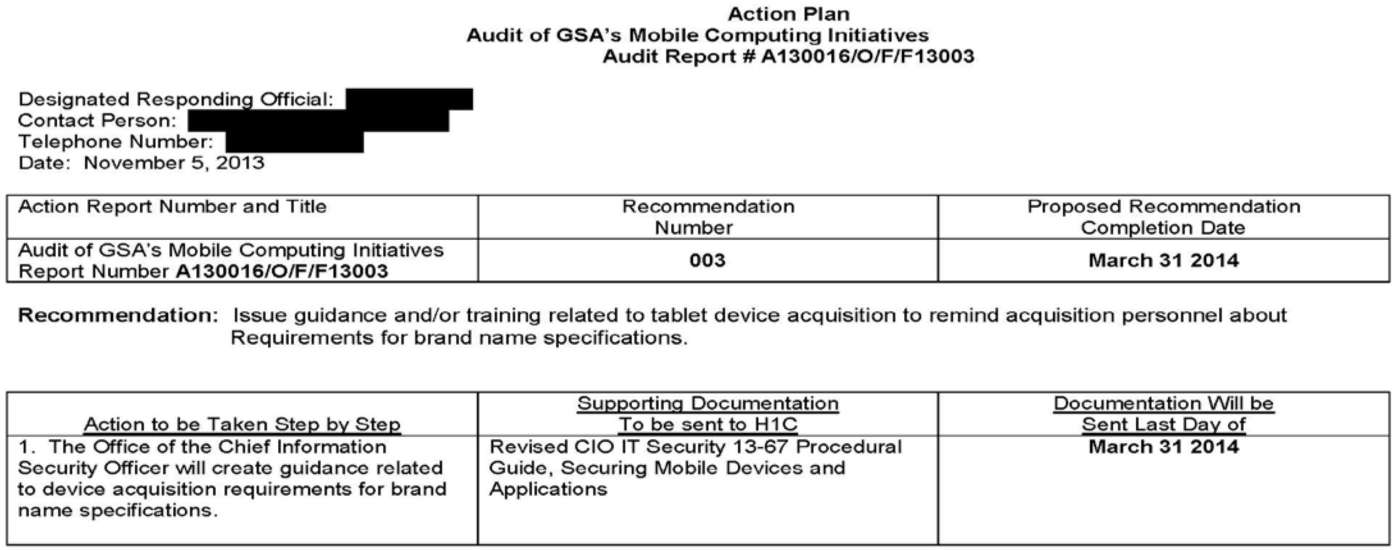
Designated Responding Official: [redacted]
Contact Person: [redacted]
Telephone Number: [redacted]
Date: November 5, 2013

Action Report Number and Title	Recommendation Number	Proposed Recommendation Completion Date
Audit of GSA's Mobile Computing Initiatives Report Number **A130016/O/F/F13003**	**002**	**June 28, 2014**

Recommendation: Ensure that currently deployed mobile applications meet the updated standards

Action to be Taken Step by Step	Supporting Documentation To be sent to H1C	Documentation Will be Sent Last Day of
1. The Office of the Chief Information Security Officer will ensure deployed mobile applications including the four (4) applications identified during the audit are reviewed to ensure compliance with the updated CIO IT Security 13-67 Procedural Guide , Securing Mobile Devices and Applications guide.	Verification of the reviews completed	**June 28, 2014**
2. Obtain updated Authority To Operate (ATO) letters for all applications reviewed, signed by the respective Authorizing Official.	Copy of all signed ATOs	**June 28, 2014**

Appendix A – Action Plan for Report Number A130016/O/F/F13003 (cont.)



Action Plan
Audit of GSA's Mobile Computing Initiatives
Audit Report # A130016/O/F/F13003

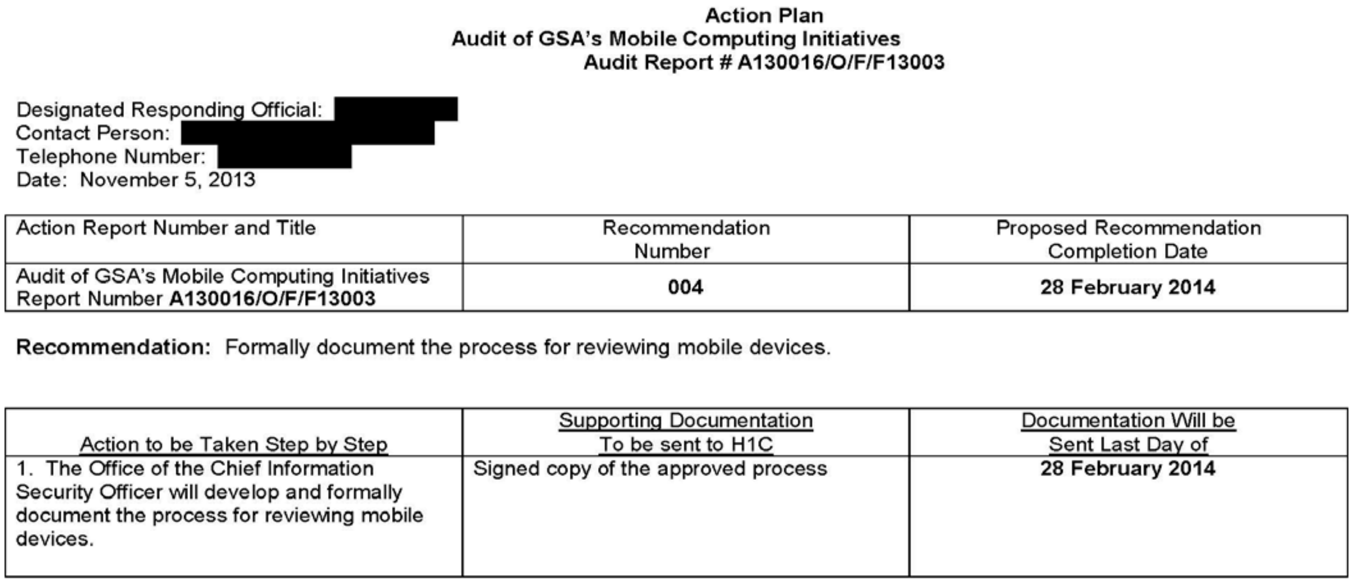
Designated Responding Official: [redacted]
Contact Person: [redacted]
Telephone Number: [redacted]
Date: November 5, 2013

Action Report Number and Title	Recommendation Number	Proposed Recommendation Completion Date
Audit of GSA's Mobile Computing Initiatives Report Number **A130016/O/F/F13003**	**003**	**March 31 2014**

Recommendation: Issue guidance and/or training related to tablet device acquisition to remind acquisition personnel about Requirements for brand name specifications.

Action to be Taken Step by Step	Supporting Documentation To be sent to H1C	Documentation Will be Sent Last Day of
1. The Office of the Chief Information Security Officer will create guidance related to device acquisition requirements for brand name specifications.	Revised CIO IT Security 13-67 Procedural Guide, Securing Mobile Devices and Applications	**March 31 2014**

Appendix A – Action Plan for Report Number A130016/O/F/F13003 (cont.)



Action Plan
Audit of GSA's Mobile Computing Initiatives
Audit Report # A130016/O/F/F13003

Designated Responding Official: [redacted]
Contact Person: [redacted]
Telephone Number: [redacted]
Date: November 5, 2013

Action Report Number and Title	Recommendation Number	Proposed Recommendation Completion Date
Audit of GSA's Mobile Computing Initiatives Report Number **A130016/O/F/F13003**	**004**	**28 February 2014**

Recommendation: Formally document the process for reviewing mobile devices.

Action to be Taken Step by Step	Supporting Documentation To be sent to H1C	Documentation Will be Sent Last Day of
1. The Office of the Chief Information Security Officer will develop and formally document the process for reviewing mobile devices.	Signed copy of the approved process	**28 February 2014**

Appendix B – Report Distribution

Chief Information Officer (I)

Senior Agency Information Security Officer (IS)

Branch Chief, GAO/IG Audit Response Division (H1C)

Audit Liaison, GSA IT (IA, ISP)

Assistant Inspector General for Auditing (JA)

Deputy Assistant IG for Investigations (JID)

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