OFFICE OF
INSPECTOR GENERAL
U.S.DEPARTMENT OF THE INTERIOR

Report No. WR-VS-GSV-0008-2010
September 22, 2010

Memorandum

To: Director, U.S. Geological Survey

Assistant Secretary for Policy, Management and Budget
(Attention: Branch Chief, Internal Control and Audit Follow-up)

From: Michael P. Colombo
Regional Manager

Subject: Verification Review of Recommendations One, Two, and Three of Evaluation Report Titled “USGS Store Not Protecting Payment Card Information” (Report No. ER-EV-GSV-0002-2009), June 2009

The Office of Inspector General has completed a verification review of three recommendations presented in the subject evaluation report. The objective of the review was to determine whether the recommendations were implemented as reported to the Office of Financial Management, Office of Policy, Management and Budget. In a memorandum dated September 28, 2009, the Office of Financial Management reported to the Office of Inspector General that all of the recommendations in the subject report had been implemented and the audit report closed.

Background

Our June 2009 evaluation report titled “USGS Store Not Protecting Payment Card Information” (Report No. ER-EV-GSV-0002-2009) made three recommendations to the U.S. Geological Survey (USGS) relating to the operation of the USGS web-based store, which was not in compliance with payment card protection standards issued by the Payment Card Industry (PCI) Security Standards Council and system security standards issued by the Department of the Interior.

In a July 8, 2009 response to the draft report, USGS concurred with all three of the recommendations. Accordingly, the Office of Inspector General considered all three of the recommendations resolved but not implemented. Based on this response, together with the information that USGS subsequently provided, the Office of Inspector General referred Recommendations 1, 2, and 3 for implementation tracking on July 22, 2009, to the Assistant Secretary for Policy, Management and Budget.

Scope and Methodology

The scope of this review was limited to determining whether USGS took action to implement the recommendations. To accomplish our objective, we reviewed the supporting documentation that USGS officials provided us relating to each of the three recommendations. We also interviewed USGS officials to gather additional information and to seek clarification on some of the information that USGS provided us.

We did not perform any site visits or conduct any detailed audit fieldwork to determine whether the underlying deficiencies that were initially identified have, in fact, been corrected. As a result, this review was not conducted in accordance with the "Government Auditing Standards," issued by the Comptroller General of the United States.

Results of the Review

Our current review found that USGS implemented all three of the recommendations.

Recommendation 1: Complete the annual self-assessment checklist for the Store.

In its September 24, 2009 response, USGS reported that it completed the PCI Self-Assessment Questionnaire (SAQ) on July 28, 2009, using the most current SAQ version provided by the PCI Security Standards Council. Our review found that USGS did in fact complete the PCI SAQ for the Store. To support whether the checklist will be completed annually, USGS stated that the SAQ has been included as part of its Fiscal Year End Closeout Process in which each item listed in the Closeout Checklist must be completed by fiscal year end. USGS provided us with the 2010 Fiscal Year End Closeout Calendar, and the SAQ is scheduled for completion between September 20 and 30, 2010. As a result, we concluded that Recommendation 1 has been resolved and implemented.

Recommendation 2: Have a certified vendor perform network scanning or obtain certification itself.

In its September 24, 2009 response, USGS stated that it used Symantec Corporation as the Approved Scanning Vendor (ASV) and provided the initial quarterly scan result conducted on September 17, 2009, in which the ASV reported that USGS was compliant. We requested and received all four of the scanning results, and each one of them reported that USGS was compliant. We conducted research on the PCI Security Standards Council Web site to verify if Symantec was a certified ASV and were able to confirm that they were. As a result, we concluded that Recommendation 2 has been resolved and implemented.

Recommendation 3: Review the [Integrated Business Solution] security plan as soon as possible and once a year thereafter.

In its September 24, 2009 response, USGS reported as part of the Certification and Accreditation process, IT Specialists who support the Store infrastructure updated the Integrated Business Solution (IBiS) System Security Plan in January 2009. The system security plan was reviewed and signed on February 2009, and was posted on the USGS internal Certification and Accreditation document management site in April 2009.

USGS provided us with the January 2009 IBiS System Security Plan that appeared to be complete. The plan includes a Record of Changes that documents the system security plan was updated in January 2009. USGS officials told us it would be reviewed on an annual basis because it was included as part of the 2010 Fiscal Year End Closeout Process and that all items on the Closeout Checklist must be completed by fiscal year end. They provided us with the fiscal year 2010 Closeout Calendar, which shows that USGS plans to review the IBiS System Security Plan between September 20 and 30, 2010. As a result, we concluded that Recommendation 3 has been resolved and implemented.

Conclusion

We informed USGS officials of the results of this review at an exit conference on September 15, 2010. The USGS officials agreed with the results of this verification review.

If you have any questions about this report, please contact me at (916) 978-5653.

cc: Liaison Officer, Assistant Secretary for Water and Science
Liaison Officer, U.S. Geological Survey
Associate Director for Geospatial Information and Chief Information Officer,
U.S. Geological Survey