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

Recommendations for the Report Titled *Information Security Weaknesses at a Core Data Center Could Expose Sensitive Data* (Report No. 2016-ITA-021)

This is a revised version of the report prepared for public release.

In recognition of Secretarial Order No. 3380, we are providing estimated costs associated with certain work products. Applying a formula involving prior salary and benefit expenses, we estimate the cost of preparing this report to be $13,000.

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

DEC 15 2020

Memorandum

To: Tonya Johnson
Deputy Chief Financial Officer and Director, Office of Financial Management

From: Nicki Miller
Regional Manager, Eastern Region

Subject: Verification Review – Recommendations for the Report Titled *Information Security Weaknesses at a Core Data Center Could Expose Sensitive Data* (Report No. 2016-ITA-021)
Report No. 2020-ER-040

The Office of Inspector General (OIG) has completed a verification review of the eight recommendations presented in the subject report. Our objective was to determine whether the Bureau of Indian Affairs (BIA) and the Office of the Chief Information Officer (OCIO) implemented the recommendations as reported to the Office of Financial Management (PFM), Office of Policy, Management and Budget. The PFM reported to the OIG that it has closed the recommendations. We concur that all recommendations have been resolved and implemented.

Background

Our report, *Information Security Weaknesses at a Core Data Center Could Expose Sensitive Data*, dated February 15, 2017, made eight recommendations designed to assist the U.S. Department of the Interior (DOI) to ensure the effectiveness of selected information technology (IT) security controls for protecting the DOI's [redacted] and the computer systems it houses from potential loss or disruption and ensuring continuity of business operations should the [redacted] experience a disaster.

The BIA and the OCIO concurred with the report's recommendations in a memorandum dated January 6, 2017, and detailed their plans to implement them. On the basis of the BIA's and the OCIO's responses to the draft report, we considered one recommendation (Recommendation 5) resolved and implemented and seven recommendations resolved but not implemented. We referred those seven recommendations (1 – 4 and 6 – 8) to the Assistant Secretary for Policy, Management and Budget to track their implementation.

Scope and Methodology

The scope of this review was limited to determining whether the BIA and the OCIO implemented the recommendations we reported. To accomplish our objective, we reviewed the supporting documentation that agency officials provided and discussed actions taken to

implement the report's eight recommendations. We did not conduct internal control testing, site visits, or fieldwork to determine whether the underlying deficiencies that were initially identified have been corrected. As a result, this review was not conducted in accordance with generally accepted government auditing standards issued by the Comptroller General of the United States or the *Quality Standards for Inspection and Evaluation* issued by the Council of the Inspectors General on Integrity and Efficiency.

Results of Review

Our current review found that the BIA's and the OCIO's actions have met the intent of resolving and implementing all eight recommendations.

Recommendation 1: Establish an ongoing process to ensure the inventory of its systems is continually updated and accurate.

Action Taken: The BIA completed the foundational activities/corrective actions associated with the OCIO's Federal Information Security Modernization Act of 2014 (FISMA) Tagging Initiative. Specifically, the BIA populated FISMA tags and applied simple network management protocol FISMA tags. In addition, it provided the OCIO with an inventory of remaining devices that were not supported for manual authorization. The OCIO provides ongoing compliance checks through weekly reporting or metrics.

The OCIO's fiscal year 2019 organizational assessment determined that the BIA and the Bureau of Indian Education (BIE) achieved a "Green Rating" (or full compliance) once 90 percent of all devices were tagged.

Recommendation 2: Install IBM BigFix agents on all applicable BIA and BIE devices.

Action Taken: The BIA used methodology provided by the DOI to identify "qualifying hosts," that do not include the BigFix agent. The Office of Information Management Technology (OIMT) developed a procedure to test and verify that IBM BigFix agents are installed and functioning properly on applicable BIA and BIE devices. For devices with malfunctioning or missing BigFix agents, the OIMT Systems Division uninstalled and reinstalled the agents.

The OCIO expects to issue a directive that will ensure the BIA and the BIE implement the BigFix agent on all devices. The draft directive uses oversight from the DOI to ensure that BigFix is installed, updated, and functioning properly.

Recommendation 3: Implement controls that identify and remove unauthorized and unsupported products from the BIA and BIE systems.

Action Taken: The OIMT developed and disseminated a restricted products list and enhanced the capabilities of the monitoring tools the Computer Incident Response Team uses. These tools use IBM BigFix, [redacted], and [redacted] to create a policy that prohibits users from executing unauthorized software programs on either network.

Recommendation 4: Ensure that critical and high-risk vulnerabilities on BIA and BIE systems are mitigated within 30 days of detection in accordance with DOI policy.

Action Taken: The OIMT, the Division of Information Security, and the Division of Information Operations developed and implemented a vulnerability remediation/mitigation standard operating procedure (SOP) to ensure critical and high-risk vulnerabilities on BIA and BIE systems are mitigated within 30 days, per DOI policy. The SOP is divided into four phases: discovery and identification, research and planning, remediation, and monitoring.

Recommendation 5: Review contracts for BIA and BIE systems managed by contractors to ensure the contract contains the appropriate Federal computer security requirements, including critical IT security controls such as vulnerability detection and mitigation.

Action Taken: The BIA reviewed the [redacted] statement of work and determined that it includes the overarching security requirements. In addition, the BIA developed a guidance document to reset expectations with the [redacted] contractor for security and privacy controls and more clearly define the deliverables and reporting requirements that support those controls. The BIA will share this document with other BIA and BIE contracting officers to use in future contracts.

Recommendation 6: Monitor contractors managing BIA and BIE systems to ensure all IT security requirements are met.

Action Taken: The BIA conducted a site visit in April 2018 with [redacted], who assured the BIA that staff members are aware of the IT security and privacy requirements described in [redacted] contract and statement of work. The BIA provided documentation that showed it monitors the IT assets comprising [redacted] for compliance with IT security requirements and vulnerability scans.

Recommendation 7: Monitor system configuration settings to ensure BIA and BIE systems remain securely configured over time.

Action Taken: The DOI established approved configuration baselines in order of precedence and enabled configuration checks for the major operating systems in use within the DOI, which uses that tool to report on compliance with those baselines.

BIA should document through the normal process and through its Risk Management function any deviation from the approved baselines for settings that cannot be implemented at the individual bureaus.

Recommendation 8: Establish an independent verification and validation function to ensure that all Federal and DOI IT security requirements are met and its data centers and the information systems they house are adequately secured.

Action Taken: The OCIO's Compliance and Audit Management Branch implemented or enhanced a number of activities, including using independent auditors to direct FISMA

compliance reviews, conducting other assessments across the DOI, and providing independent oversight and access for the DOI's Cloud Program to ensure the necessary authorizations are monitored and compliant.

Conclusion

We informed BIA and OCIO officials of the results of this review on September 10, 2020. We found no issues with the BIA's or OCIO's implemented actions, and neither bureau requested an exit conference.

cc: Andrea Brandon Deputy Assistant Secretary for The Office of Policy, Management and Budget
Chadrick Minnifield, Division Chief, Internal Control and Audit Follow-Up, Office of Financial Management
Richard Westmark, Chief, Compliance and Audit Management Branch, Office of the Chief Information Officer
Tara Sweeney, Assistant Secretary, Indian Affairs
Richard Myers, Chief of Staff, Assistant Secretary – Indian Affairs
Karen Frejo, Audit Liaison Officer, Bureau of Indian Affairs
Spike Bighorn, Audit Liaison Officer, Bureau of Indian Education
Alexis Vann, Audit Liaison Officer, Office of Financial Management
Preston Wong, Audit Liaison Officer, Office of Financial Management
PFM ICAF Email
OCIO Email

Report Fraud, Waste, and Mismanagement

Fraud, waste, and mismanagement in Government concern everyone: Office of Inspector General staff, departmental employees, and the general public. We actively solicit allegations of any inefficient and wasteful practices, fraud, and mismanagement related to departmental or Insular Area programs and operations. You can report allegations to us in several ways.

By Internet: www.doioig.gov

By Phone: 24-Hour Toll Free: 800-424-5081
Washington Metro Area: 202-208-5300

By Fax: 703-487-5402

By Mail: U.S. Department of the Interior
Office of Inspector General
Mail Stop 4428 MIB
1849 C Street, NW.
Washington, DC 20240