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

Recommendations 1, 2, 5, and 6 for the Evaluation Report Titled *U.S. Department of the Interior's Continuous Diagnostics and Mitigation Program Not Yet Capable of Providing Complete Information for Enterprise Risk Determinations* (Report No. ISD-IN-MOA-0004-2014-I)

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

Memorandum

SEP 2 3 2020

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

From: Nicki Miller *Nicki Miller*
           Eastern Regional Manager for Audits, Inspections, and Evaluations

Subject: Verification Review – Recommendations 1, 2, 5, and 6 for the Evaluation Report
           titled *U.S. Department of the Interior's Continuous Diagnostics and Mitigation
           Program Not Yet Capable of Providing Complete Information for Enterprise Risk
           Determinations*, Report No. ISD-IN-MOA-0004-2014-I
           Report No. 2020-ER-048

        The Office of Inspector General has completed a verification review of Recommendations
1, 2, 5, and 6 presented in the subject report. Recommendations 3 and 4 of the report remain
open. Our objective was to determine whether the Office of the Chief of Information Officer
(OCIO) implemented the recommendations as reported to the Office of Financial Management
(PFM), Office of Policy, Management and Budget. In documents sent on June 18, 2020, the PFM
reported that it had closed all four recommendations. After our review, we concur that
Recommendations 1, 2, 5, and 6 have been resolved and implemented.

Background

        Our September 2016 evaluation report, *U.S. Department of the Interior's Continuous
Diagnostics and Mitigation Program Not Yet Capable of Providing Complete Information for
Enterprise Risk Determinations*, made six recommendations to assist the OCIO work toward an
improved cybersecurity environment and a raised level of risk awareness.

Scope and Methodology

        We limited the scope of this review to determining whether the OCIO took sufficient
action to implement Recommendations 1, 2, 5, and 6. To accomplish our objective, we
interviewed OCIO staff and reviewed the PFM's documentation supporting its closure of the
four recommendations as well as additional documentation that the OCIO provided to us upon
request.

        We did not test internal controls, perform any site visits, or conduct fieldwork to
determine whether the OCIO had corrected the underlying deficiencies that were initially
identified. 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

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

Action Taken: The U.S. Department of the Interior (DOI) Information Management and Technology Leadership Team (IMTLT) established three processes to continually monitor the Department's IT assets and infrastructure. The IMTLT:

1. Implemented FISMA (Federal Information Security Modernization Act of 2014) tagging standards and required implementation in all DOI bureaus and offices on all applicable network-connected devices.

2. Purchased the ███████████ to serve as the Department's Hardware Asset Management (HWAM) solution.

3. Purchased and uses ███████████ that aggregates network-connected devices and monitors for configuration compliance across DOI networks to maintain overall cybersecurity.

Together, █████████████████████████████ enable the OCIO to perform the Continuous Diagnostics and Mitigation function. The OCIO monitors these systems continuously, estimating coverage of the DOI network at an acceptable 95 percent and asserting that these programs were achieving established objectives.

Therefore, we determined that the requirements for Recommendation 1 are met and this recommendation is resolved and implemented.

Recommendation 2: Enforce the requirement that all bureaus are to install IBM BigFix agents on all applicable devices to support IBM BigFix as an enterprise hardware inventory solution.

Action Taken: The IMTLT demonstrated work toward a mandatory requirement for the employment of BigFix agents on applicable DOI network-connected devices.

After our review, we determined that the requirements for Recommendation 2 are met and this recommendation is resolved and implemented.

Recommendation 5: Establish a departmentwide configuration baseline for computers not covered by [the] USGCB [U.S. Government Configuration Baseline] that includes a waiver application and approval process.

Action Taken: The IMTLT published policy directing the use of Security Technical Implementation Guides on all applicable DOI devices, thus achieving implementation of configuration baselines across the DOI. Furthermore, the OCIO demonstrated a waiver application and approval process for non-USGCB systems.

After our review, we find that the requirements for Recommendation 5 are met and this recommendation is resolved and implemented.

Recommendation 6: Monitor computer operating system configuration settings to ensure computers remain securely configured.

Action Taken: Using reports generated through the systems named in Recommendation 1, IT managers identify systems with unauthorized security settings. This process allows IT managers to implement remedial action on individual systems.

After our review, we find that the requirements for Recommendation 6 are met and this recommendation is resolved and implemented.

Conclusion

We consider Recommendations 1, 2, 5, and 6 resolved and implemented. We informed OCIO officials of the results of this review on September 3, 2020.

We would like to thank the OCIO for providing us the information requested during our review. If you have questions about this verification review, please contact me at 202-208-5745.

cc: Richard Westmark, Audit Liaison, Office of the Chief Information Officer
        Rebecca Bageant, Audit Liaison, U.S. Geological Survey
        Pam Clemens, Audit Liaison, U.S. Bureau of Reclamation
        Linh Luu, Audit Liaison, U.S. Bureau of Safety and Environmental Enforcement

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	