MEMORANDUM

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

EVALUATION OF THE U.S. DEPARTMENT OF THE INTERIOR'S CYBERSECURITY PRACTICES FOR PROTECTING CRITICAL INFRASTRUCTURE – [redacted], AND [redacted]

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

Report No.: 2017-ITA-023-A July 2018

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

Memorandum

JUL 12 2018

To: Brenda Burman
Commissioner, U.S. Bureau of Reclamation

From: Jefferson Gilkeson
Director, Information Technology Audits
Office of Audits, Inspections, and Evaluations

Subject: Closeout Memorandum – Evaluation of the U.S. Department of the Interior's Cybersecurity Practices for Protecting Critical Infrastructure – [redacted], and [redacted]
Report No. 2017-ITA-023-A

We completed our work for the second part of our series to evaluate the U.S. Bureau of Reclamation's (USBR's) practices for protecting critical hydropower dams from emerging cyber threats.[1] The second part of this evaluation was limited to the USBR's [redacted]) system. The [redacted] is an industrial control system that provides monitoring, alarming, and process control to ensure the safe and reliable operations of the water and power facilities for the [redacted], and [redacted]. We determined that additional efforts on this project are not needed. Further, the recommendations in our first report in this series – to improve the USBR's account management and personnel security practices – apply to all of USBR's hydropower dams.

Our technical analysis of data collected from the [redacted] found several conditions that helped reduce [redacted] risk of compromise from external cyber threats. Specifically, the [redacted] was built on private IP address space, which helps protect it from external cyber threats. Our review of network traffic did not identify any significant anomalies or indicators of compromise. We did not identify malware or other indicators of compromise during our analysis of memory from 12 key [redacted] computers. We also found that the USBR has implemented controls to help prevent the introduction of malware infections from external media such as USB devices. As such, we determined that additional efforts on this project are not warranted.

We appreciate the cooperation and assistance provided by your staff during our survey work. If you have any questions regarding this memorandum, please contact me at 703-487-5357.

[1] *U.S. Bureau of Reclamation Selected Hydropower Dams at Increased Risk From Insider Threats* (Report No. 2017-ITA-023), issued June 7, 2018.

cc: Sylvia Burns, Chief Information Officer
Lawrence Ruffin, Chief Information Security Officer
Joyce Harris, Bureau of Reclamation Chief Information Security Officer
Brenda Albery, Bureau of Reclamation Audit Liaison
Matthew Diem, Bureau of Reclamation Audit Liaison
Douglas Glenn, Director, Office of Financial Management
Allen Lawrence, Division Chief, Internal Controls and Audit Followup
Richard Westmark, Chief, Compliance and Audit Management Branch
Peter Brownell, Audit Liaison Officer, Compliance and Audit Management Branch
Alexandra Lampros, Audit Liaison Officer, Office of Financial Management
Nancy Thomas, Audit Liaison Officer, Office of Financial Management

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