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

Inspection of the DATA Act Internal Controls for the U.S. Department of the Interior, Interior Business Center, for the First Quarter of FY 2021

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

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

JUN 23 2022

Memorandum

To: Byron M. Adkins, Jr.
Director, Interior Business Center

Wendell Bazemore
Associate Director, Financial Management
Interior Business Center

Matthew Costello
Associate Director, Enterprise Management
Interior Business Center

From: Kathleen Sedney
Assistant Inspector General for Audits, Inspections, and Evaluations

Subject: Final Inspection Report – *Inspection of the DATA Act Internal Controls for the U.S. Department of the Interior, Interior Business Center, for the First Quarter of FY 2021*
Report No. 2021–FIN–024

This report presents the results of our inspection of the U.S. Department of the Interior (DOI) Interior Business Center's (IBC's) 2021 internal controls placed over the data management and processes used to report financial and award data to USAspending.gov.

Why We Conducted This Inspection

The Digital Accountability and Transparency Act of 2014 (DATA Act) requires a series of oversight reports by Federal agency Offices of Inspector General (OIGs), including assessments of the internal controls over DATA Act submissions.[1] We chose to review these specific internal controls and provide our results to OIGs for external IBC customers so that those OIGs could use the results to determine the nature, extent, and timing of their own audit procedures and perform those procedures.

The IBC is a Federal Shared Service Provider (FSSP) that submits DATA Act data to the Treasury Broker for external clients. Because the IBC is an office within the DOI, we chose to review the IBC's respective FSSP internal controls over the DATA Act submissions for the OIGs of the IBC's external customers. Each IBC DATA Act client OIG will perform its own DATA Act audit, whether completed by the OIG or contracted to an outside audit entity. We

[1] Data Act submissions are specific data elements that agencies must report to the Treasury Broker under the Data Act. The Treasury Broker is a tool developed by the U.S. Department of the Treasury to allow agencies to submit the required data in a standardized format for publication on USAspending.gov.

believe that our inspection will reduce the need for other OIGs to complete an internal controls assessment of the IBC.

What We Reviewed

The objective of our inspection was to determine and assess the internal controls the IBC has in place over the preparation and submission of client data required by the DATA Act. We assessed those internal controls to determine if they complied with the U.S. Government Accountability Office's (GAO's) *Standards for Internal Control in the Federal Government* (*Green Book*).

We did not expound on internal controls that covered both DATA Act services and other functions within the IBC or the IBC as a complete entity. Instead, we examined the internal controls over DATA Act services only. We did this to avoid duplicating any previous work completed by KPMG in the SSAE 18 SOC 1 Report[2] and meet the guidelines within section 300 of the *CIGIE FAEC Inspectors General Guide to Compliance under the DATA Act* (December 2020) (DATA Act Audit Guide).

See Attachment 1 for the inspection's scope and methodology. Attachment 2 assesses the IBC's internal control system per the *Green Book*'s 5 components and 17 principles.

What We Found

We found the IBC generally had necessary and effective internal controls in place over the preparation and submission of client data, as required by the DATA Act. Specifically, we found the IBC implemented all 5 internal control components and 17 internal control principles outlined in the *Green Book*.[3] However, we did find that the IBC has not yet completed an Enterprise Risk Management (ERM) program. An ERM program is a discipline designed to effectively manage risk, identify challenges early, and bring them to the attention of agency leadership to develop appropriate solutions. Risk assessment is also a significant component of internal control, in which management must assess the risk facing the entity as it seeks to achieve its objectives. Although the IBC has developed other policies and practices to incorporate the internal control principles related to risk, the development and implementation of a robust ERM program ensures that risks are appropriately identified, analyzed, and responded to.[4]

Furthermore, according to the OMB's Memorandum, M-16-17, *OMB Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control*, Federal agencies are required to "implement an [ERM] capability coordinated with the strategic planning and strategic review process established by [the Government Performance and Results

[2] [redacted] Federal Financials - Report on the U.S. Department of the Interior's Description of Its [redacted] Federal Financials System and the Suitability of the Design and Operating Effectiveness of Its Controls (SSAE 18 SOC 1® – Type 2 Report), For the Period July 1, 2019 to June 30, 2020 for [redacted] Federal Financials.

[3] See Attachment 2 for a full description of what we found in our assessment of each component and principle.

[4] In addition, the CIGIE FAEC's DATA Act Audit Guide identifies an ERM program as a topic to consider when assessing internal controls. An ERM program improves mission delivery, reduces costs, and focuses corrective actions toward key risks.

Act Modernization Act of 2010] and the internal controls processes required by [the Federal Managers Financial Integrity Act of 1982] and [the GAO's] *Green Book*."

The IBC has been collaborating with the Office of Planning and Performance Management to complete the DOI's ERM program since 2019.[5] The IBC's ability to address this issue, however, is limited because it must wait for the DOI to complete its own ERM program. This is because the DOI must identify the overarching risks facing the agency before those can be cascaded down to the bureaus. In the interim, the IBC is encouraged to consider any unique risk factors it may be able to identify and put processes in place so that it can act promptly once the DOI completes its own work. The IBC responded to a draft of this report and stated that it concurred and that it "will have a defined risk appetite statement, a prioritized risk register, and an enterprise-wide risk profile" by June 30, 2022. See Attachment 3 on page 15 for the IBC's full response.

We will notify Congress about our findings, and we will summarize this work in our next *Semiannual Report to Congress,* as required by law. We will also post a public version of this report on our website.

If you have any questions, please contact me or Nicki Miller, Acting Deputy Assistant Inspector General for Audits, Inspections, and Evaluations, at 202-208-5745.

Attachments

[5] *U.S. Department of the Interior DATA Act Submission For First Quarter FY 2019* (Report No. 2019–FIN–043), dated November 2019.

Attachment 1: Scope and Methodology

Scope

The scope of our inspection covered the Interior Business Center's (IBC's) internal controls over Digital Accountability and Transparency Act of 2014 (DATA Act) services for clients for first quarter fiscal year (FY) 2021. We reviewed the IBC's implementation of the 5 components and 17 principles of the U.S. Government Accountability Office's *Standards for Internal Control in the Federal Government*.

KPMG covered the [redacted] Federal Financials system's information system controls in its *Report on the U.S. Department of the Interior's Description of Its* [redacted] *Federal Financials System and the Suitability of the Design and Operating Effectiveness of Its Controls (SSAE 18 SOC 1® – Type 2 Report), For the Period July 1, 2019 to June 30, 2020 for* [redacted] *Federal Financials financial audit of the U.S. Department of the Interior (DOI)*, and we did not duplicate those efforts. Therefore, we did not assess the [redacted] Federal Financials system and its Application Controls.

Our assessment focused on the IBC's DATA Act services and processing of client Office of Inspector General data. We determined how and whether the IBC's existing internal controls applied to the DATA Act services as outlined and required within Section 300 of the DATA Act Audit Guide. We accomplished this by determining how the IBC's internal controls met the requirements within each internal control principle established in the U.S. Government Accountability Office's *Standards for Internal Control* and how each covered the DATA Act internal control requirements for Federal Shared Service Providers.

Methodology

We conducted our inspection in accordance with the *Quality Standards for Inspection and Evaluation* as put forth by the Council of the Inspectors General on Integrity and Efficiency (CIGIE). We did not test the implementation, design, or operating effectiveness of the controls. We believe that the work performed provides a reasonable basis for our conclusions and recommendations.

To accomplish our objective, we:

- Reviewed relevant information used to prepare our previous IBC DATA Act Internal Controls Report from FY 2017

- Identified and reviewed Office of Management and Budget, CIGIE, DOI, and IBC guidance, policies, and procedures related to the IBC's internal controls process

- Obtained, reviewed, and assessed the IBC's responses and support to our internal control questionnaire

- Assessed the internal controls over DATA Act processes during a walkthrough of the IBC's systems and processes via the Microsoft Teams application

Attachment 2: OIG's Assessment of the IBC's Internal Controls

We sent a questionnaire, reviewed the questions against supporting documentation, and conducted a walkthrough to assess how the Interior Business Center (IBC) addressed each principle of the U.S. Government Accountability Office's *Standards for Internal Control* (*Green Book*). The following table summarizes our assessment and the IBC's practices for each principle.

Component 1 – Control Environment

The control environment is the foundation for an internal control system. It provides the discipline and structure, which affect the overall quality of internal control. It influences how objectives are defined and how control activities are structured. The oversight body and management establish and maintain an environment throughout the entity that sets a positive attitude toward internal control.

Principle	OIG Assessment of IBC Policies, Practices, and Procedures
Principle 1 – The oversight body and management should demonstrate a commitment to integrity and ethical values	• The IBC sets forth ethical guidance based on Secretarial Order 3375, *Improving the Department of the Interior's Ethics Programs through Consolidation,* implemented on August 28, 2019. The purposes of this Order are to a) realign the reporting structure for ethics personnel in the Department of the Interior (DOI) into the DOI Ethics Office and b) clarify roles and responsibilities regarding the ethics program for DOI employees, program managers, and ethics officials. IBC guidance is also included on IBCnet's Ethics and Integrity page. The page identifies the 14 Principles of Ethical Conduct for Employees, Merit System Principles, and Prohibited Personnel Practices and has contact information for the DOI Ethics Office, the Office of Government Ethics, the Merit Systems Protection Board, and the Federal Labor Relations Authority. Annual Ethics training is required only for those who file an annual financial disclosure report. • Based on our assessment of the documentation and information provided, we believe the IBC is sufficiently meeting the requirements of Principle 1.
Principle 2 – The oversight body should oversee the entity's internal control system	• KPMG provides external oversight for the IBC's internal controls. KPMG performs an annual report that evaluates the design and implementation of internal controls for the [redacted] financial accounting system (the SOC 1 Report). • The IBC uses the SOC 1 Report to be made aware of any internal control weaknesses. • Based on our assessment of the documentation and information provided, we believe that the IBC is sufficiently meeting the requirements of Principle 2.

Principle	OIG Assessment of IBC Policies, Practices, and Procedures
Principle 3 – Management should establish an organizational structure, assign responsibility, and delegate authority to achieve the entity's objectives	• The IBC has an organizational chart that establishes the IBC organizational structure, the responsibilities assigned to each person, and the authority delegated to each person. • The IBC informs staff of DATA Act requirements and system changes to the Treasury Broker that are passed down from The Treasury DATA Act Program Management Office (PMO). This information, along with internal control corrections, is addressed during the IBC's monthly Corrective Action Plan (CAP) with IBC leadership and management. • Based on our assessment of the documentation and information provided, we believe that the IBC is sufficiently meeting the requirements of Principle 3.
Principle 4 – Management should demonstrate a commitment to recruit, develop, and retain competent individuals	• The IBC, within its organizational chart and leadership biographies, has displayed a framework and standard for expectations of competencies for its leadership roles. The IBC has a formal succession and contingency plan, as well as a workforce plan for management roles. • The IBC also has performance standards for employees that communicate expectations of performance and conduct. Employees are rated annually on these performance standards. • Based on our assessment of the documentation and information provided, we believe that the IBC is sufficiently meeting the requirements of Principle 4.
Principle 5 – Management should evaluate performance and hold individuals accountable for their internal control responsibilities	• The IBC bases its ethical guidelines on the guidance set in Secretarial Order 3375. IBC guidance is also included on IBCnet's Ethics and Integrity page. The page identifies the 14 Principles of Ethical Conduct for Employees, Merit System Principles, and Prohibited Personnel Practices and has contact information for the DOI Ethics Office, the Office of Government Ethics, the Merit Systems Protection Board, and the Federal Labor Relations Authority. Annual Ethics training is required only for those who file an annual financial disclosure report. • The IBC also has performance standards for employees that that communicate expectations of performance and conduct. Employees are rated annually on these performance standards. • Based on our assessment of the documentation and information provided, the IBC is effectively using ethical guidance and performance standards and reviews to meet the requirements of Principle 5.

Component 2 – Risk Assessment

Having established an effective control environment, management assesses the risks facing the entity as it seeks to achieve its objectives. This assessment provides the basis for developing appropriate risk responses. Management assesses the risks the entity faces from both external and internal sources.

Principle	OIG Assessment of IBC Policies, Practices, and Procedures
Principle 6 – Management should define objectives clearly to enable the identification of risks and define risk tolerances	• The IBC is working with the Office of Planning and Performance Management to establish a formal Enterprise Risk Management (ERM) program for all the DOI, but no ERM program is currently implemented. • The IBC has identified minimal risks within the DATA Act Process as mapped out in the [redacted] Federal Financials (OFF) 133 DATA Act Process document indicating that permissions are required to be granted access to the OFF system and the Treasury Broker. In addition, risk tolerance is at a minimum within the DATA Act process because it was designed to only generate the necessary DATA Act files and to run warning and error reports without manipulating the client data during the process. • The IBC provided written policy and practices to show how it met the requirements in Principle 6 in lieu of an ERM program by completing an annual risk assessment per OMB Circular A-123, providing its Control and Compliance Program Policy, and through its annual SOC 1 Report compliance. Although implementation of an ERM program has not been completed, based on our assessment of the documentation and information provided, we believe that the IBC is sufficiently meeting the requirements of Principle 6.
Principle 7 – Management should identify, analyze, and respond to risks related to achieving the defined objectives	• The IBC relies on the processes described in its Financial Management Directorate Configuration Management Plan (FMD CMP) to identify, analyze, and respond to risks. It is important to note that the client's Senior Accountable Official's (SAO's) certification for data quality within the Treasury Broker is the client's responsibility and must align with the client's Data Quality Plan. • The IBC performs OFF system testing when [redacted] provides system patches and new releases to ensure that the processes execute properly, and that data are generated in the correct format. • Based on our assessment of the documentation and information provided, we believe that the IBC is sufficiently meeting the requirements of Principle 7.

Principle	OIG Assessment of IBC Policies, Practices, and Procedures
Principle 8 – Management should consider the potential for fraud when identifying, analyzing, and responding to risks	• The DOI's Internal Control and Audit Follow-up Handbook and the DOI Financial Management Memorandum (FMM) 2021-005 provide the requirements to lower fraud risk. For example, the FMM requires annual training in preventing, detecting, and responding to fraud. • The DATA Act Process document demonstrates a need for permissions to be granted access to the OFF system and the Treasury Broker within the MAX Application. It is designed for generating the necessary DATA Act files and runs warning and error reports with no manipulation of client data in the process. • We conducted a walkthrough and observed that the process demonstrated matched the process documentation. • Based on our assessment of the documentation and information provided, we believe that the IBC is sufficiently meeting the requirements of Principle 8.
Principle 9 – Management should identify, analyze, and respond to significant changes that could impact the internal control system	• According to the IBC officials, they maintain constant situational awareness of any necessary changes issued by Treasury OMB regarding DATA Act data management and reporting. For example, Treasury publishes the standard reporting due dates on its website for Federal agencies. Any reporting changes are communicated to the clients via email and monthly [redacted] clients support meetings. • During our walkthrough, we observed the IBC's process of using client data to generate error and warning reports from the Treasury Broker. The IBC demonstrated how the generated error and warning reports indicate when a data element from client data does not match to the Treasury broker. The error and warning reports are then given to the client to correct those data elements, which enhances the clarity and consistency of reported data. • Based on our assessment of the documentation and information provided, we believe that the IBC is sufficiently meeting the requirements of Principle 9.

Component 3 – Control Activities

Control activities are the actions management establishes through policies and procedures to achieve objectives and respond to risks in the internal control system, which includes the entity's information system.

Principle	OIG Assessment of IBC Policies, Practices, and Procedures
Principle 10 – Management should design control activities to achieve objectives and respond to risks	• The IBC's FMD CMP describes the control activities designed to achieve their objectives and respond to risks. For example, the IBC performs OFF system testing when [redacted] provides system patches and new releases to ensure that the processes execute properly, and that accurate data are generated in the correct reporting format. • KPMG tests the design and operating effectives of these controls in its annual SOC 1 report. • According to the IBC, it also conducts internal controls reviews, which are reported to the IBC leadership monthly in its CAP. Through a collaborative effort, the IBC works to resolve the internal control review findings in these CAP meetings. • Based on our assessment of the documentation and information provided, we believe that the IBC is sufficiently meeting the requirements of Principle 10.
Principle 11 – Management should design the entity's information system and related control activities to achieve objectives and respond to risks	• The IBC's information system controls for Shared Service Provider services are tested by KPMG in its annual SOC 1 report. • During our walkthrough, we observed various information system controls. For example, incorrect data are flagged within OFF (the only system the IBC uses to upload and generate DATA Act files). We noted that the system has the ability to generate warnings and error reports. • Based on our assessment of the documentation and information provided, we believe that the IBC is sufficiently meeting the requirements of Principle 11.

Principle	OIG Assessment of IBC Policies, Practices, and Procedures
Principle 12 – Management should implement control activities through policies	• The DATA Act and the DATA Act Audit Guide dictate the control activities for DATA Act services. • According to its policy, the IBC does not manipulate any client data, and an IBC SAO is not required because the client SAO is ultimately responsible for certifying its own data within the Treasury Broker. The IBC policy states that DATA Act files generated within OFF are packaged together with any warnings and error reports and sent to the client SAO for review, correction, and approval. Policy states that the IBC should not make any data corrections; corrections are the responsibility of the client. According to the IBC, it also conducts internal controls reviews, which are reported to IBC leadership monthly in its CAP. Through a collaborative effort, the IBC team works to resolve the internal control review findings in these CAP meetings. • We conducted a walkthrough of the IBC's DATA Act preparation and reporting process within OFF and the Treasury Broker and verified that the controls described in the DATA Act Audit Guide and IBC policy appeared to be implemented. • Based on our assessment of the documentation and information provided, we believe that the IBC is sufficiently meeting the requirements of Principle 12.

Component 4 – Information and Communication

Management uses quality information to support the internal control system. Effective information and communication are vital for an entity to achieve its objectives. Entity management needs access to relevant and reliable communication related to internal as well as external events.

Principle	OIG Assessment of IBC Policies, Practices, and Procedures
Principle 13 – Management should use quality information to achieve the entity's objectives	• The DATA Act and the DATA Act Audit Guide provide the policy and guidance for controls over DATA Act data to ensure quality and consistency of data across the Federal Government. The ultimate responsibility for providing and ensuring quality data lies with the client that provides the DATA Act data to the IBC. • It is key for Federal agencies to provide quality data to the Treasury Broker so that accurate award and financial information is available to the public. The IBC assists its DATA Act clients in reaching this goal by providing DATA Act preparation services. We performed a walkthrough of the IBC's DATA Act preparation services and observed that the IBC generates DATA Act files within its OFF system, submits those files to the Treasury Broker on a test basis to obtain error and warning reports, and then provides the DATA Act files and error and warning reports to the client SAO. The client SAO will then resolve error and warning reports, as needed. If the client SAO requires assistance in resolving the error and warning reports, the IBC will assist the client. Once the error and warning reports are resolved, and the SAO approves, the SAO or the IBC will submit the files to the Treasury Broker, depending on the client agreement. Regardless of whether the client or the IBC submits the data to the Treasury Broker on behalf of the client, it is the client SAO's responsibility to log into the Treasury Broker and certify the data submission. • Based on our assessment of the documentation and information provided, we believe that the IBC is sufficiently meeting the requirements of Principle 13.

Principle	OIG Assessment of IBC Policies, Practices, and Procedures
Principle 14 – Management should internally communicate the necessary quality information to achieve the entity's objectives	• The IBC participates in monthly Treasury DATA Act meetings, where relevant updates and information are shared. In addition, the IBC receives the Broker Release Notes provided by Treasury that detail system changes made to the Treasury Broker relevant to reporting. This information is then communicated by the meeting attendees through internal monthly meetings. • Also, accountants will receive error notifications in OFF for any missing data when running a request to create DATA Act files. Errors are then reported to the Financial Support group for system updates to resolve the errors. For errors or warnings received during the data submission process at the Treasury Broker, the Broker will generate an error or warning report. The Treasury Broker error and warning reports are given to the client SAO to resolve. If the client SAO requires assistance, the IBC will aid the client to resolve the errors and warnings, as needed. • During our walkthrough, we observed a demonstration of these processes. • Based on our assessment of the documentation and information provided, we believe that the IBC is sufficiently meeting the requirements of Principle 14.
Principle 15 – Management should externally communicate the necessary quality information to achieve the entity's objectives	• The IBC's external communications, which take place between the IBC, the Treasury Broker, and the client, are performed through updates on Treasury DATA Act Program Management Office's website and discussed in monthly [redacted] client support meetings. • During our walkthrough, we observed a demonstration of an example of a DATA Act data submission to the Treasury Broker. The process includes two steps: The DATA Act files are uploaded to the Broker, where they are validated, and any warning and error message is exported for delivery to the client and an email message is created and sent to the client notifying them the file has been uploaded to the Broker and that warnings or errors may need validation. The client—alone or in coordination with the IBC's functional support group—then resolves these validation issues. • Based on our assessment of the documentation and information provided, we believe that the IBC is sufficiently meeting the requirements of Principle 15.

Component 5 – Monitoring

Internal control is a dynamic process that has to be adapted continually to the risks and changes an entity faces, monitoring of the internal control system is essential in helping internal control remain aligned with changing objectives, environment, laws, resources, and risks. Internal controls monitoring assesses the quality of performance over time and promptly resolves the findings of audits and other reviews. Corrective actions are a necessary complement to control activities to achieve objectives.

Principle	OIG Assessment of IBC Policies, Practices, and Procedures
Principle 16 – Management should establish and operate monitoring activities to monitor the internal control system and evaluate the results	• The internal controls for monitoring within OFF and the Treasury Broker, are warnings and error reports directly tied to DATA Act services. The FMD CMP coupled with the IBC's OFF system testing are the two main functions for monitoring and remediation of other or larger system issues. • Treasury has an internal mechanism to monitor the Broker and provides information for necessary updates. The IBC monitors Treasury's website so that changes to OFF can be executed in parallel. This ensures that the data, when submitted, are accepted properly by the Treasury Broker and that any error or warning reports are accurate for the client's ultimate correction. • KPMG conducts an annual evaluation of the internal controls over the OFF system. • Based on our assessment of the documentation and information provided, we believe that the IBC is sufficiently meeting the requirements of Principle 16.
Principle 17 – Management should remediate identified internal control deficiencies on a timely basis	• The FMD CMP includes key processes for remediation related to Configuration Management and Change Control Process. For example, the Treasury Broker will generate error and warning reports. The client is responsible for investigating and correcting errors and warnings. • According to the officials we spoke with in our walkthrough, the IBC performs OFF system testing when [redacted] provides system patches and new releases. According to a response to our questionnaire, received from an IBC official, the IBC also implements system updates when Treasury makes changes to the Treasury Broker. • Based on our assessment of the documentation and information provided, we believe that the IBC is sufficiently meeting the requirements of Principle 17.

Attachment 3: Response to Draft Report

The U.S. Department of the Interior's response to our draft report follows on page 16.

United States Department of the Interior

INTERIOR BUSINESS CENTER
Washington, DC 20240

Memorandum

To: Kathleen R. Sedney
Assistant Inspector General for Audits, Inspections, and Evaluations
Office of Inspector General (OIG)

From: Byron M. Adkins, Jr.
Director

BYRON ADKINS Digitally signed by BYRON ADKINS Date: 2022.04.11 09:53:26 -04'00'

Wendell Bazemore
Associate Director, Financial Management

WENDELL BAZEMORE Digitally signed by WENDELL BAZEMORE Date: 2022.04.11 08:33:27 -04'00'

Matthew Costello
Associate Director, Enterprise Management

MATTHEW COSTELLO Digitally signed by MATTHEW COSTELLO Date: 2022.04.11 08:45:31 -04'00'

Subject: Response to Draft Inspection Report – *Inspection of the DATA Act Internal Controls for the U.S. Department of the Interior, Interior Business Center, for the First Quarter of FY 2021* (Report No. 2021-FIN-024)

On March 31, 2022, the Interior Business Center (IBC) received your draft inspection report, *Inspection of the DATA Act Internal Controls for the U.S. Department of the Interior, Interior Business Center, for the First Quarter of FY 2021* (Report No. 2021-FIN-024). This memorandum provides IBC's comments on and action plan for responding to this report.

Overall, we agree with your finding that IBC generally had necessary and effective internal controls in place over the preparation and submission of client data, as required by the DATA Act. Also, we agree that IBC implemented all five internal control components and 17 internal control principles outlined in the U.S. Government Accountability Office's *Standards for Internal Control in the Federal Government,* except that IBC had not yet completed an Enterprise Risk Management (ERM) Program.

Department of the Interior (DOI) OIG Recommendation – IBC should consider any unique risk factors it may be able to identify and put processes in place so that it can act promptly once DOI completes its own ERM program.

- **Response:** The Interior Business Center concurs with the recommendation. We have been working with DOI on implementing an ERM program and have the infrastructure for ERM that includes an executive ERM Council and Working Groups with representation from each of our directorates. Our comprehensive approach to risk management provides executive leadership and coordinated IBC efforts (program and project) to effectively apply the ERM framework and policy to manage risk. The IBC ERM program works directly with the DOI ERM Program led by the Office of

Performance and Planning Management (PPP) to ensure that our efforts are consistent and will integrate into DOI ERM efforts.

- **Corrective Action:** In coordination with DOI PPP guidance and timelines, the IBC ERM Program will have a defined risk appetite statement, a prioritized risk register, and an enterprise-wide risk profile.
- **Target Completion Date:** June 30, 2022
- **Responsible Official:** Matthew Costello, Associate Director, Enterprise Management

Please contact Ted Aymami at [redacted] or [redacted]@ibc.doi.gov if you have comments or questions.

Attachments

cc: Jacqueline M. Jones, Deputy Assistant Secretary for Administrative Services

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

REPORT FRAUD, WASTE, ABUSE, AND MISMANAGEMENT

The Office of Inspector General (OIG) provides independent oversight and promotes integrity and accountability in the programs and operations of the U.S. Department of the Interior (DOI). One way we achieve this mission is by working with the people who contact us through our hotline.

If you wish to file a complaint about potential fraud, waste, abuse, or mismanagement in the DOI, please visit the OIG's online hotline at **www.doioig.gov/hotline** or call the OIG hotline's toll-free number: **1-800-424-5081**

Who Can Report?

Anyone with knowledge of potential fraud, waste, abuse, misconduct, or mismanagement involving the DOI should contact the OIG hotline. This includes knowledge of potential misuse involving DOI grants and contracts.

How Does it Help?

Every day, DOI employees and non-employees alike contact the OIG, and the information they share can lead to reviews and investigations that result in accountability and positive change for the DOI, its employees, and the public.

Am I protected?

Complainants may request confidentiality. The Privacy Act, the Inspector General Act, and other applicable laws protect complainants. Section 7(b) of the Inspector General Act of 1978 states that the Inspector General shall not disclose the identity of a DOI employee who reports an allegation or provides information without the employee's consent, unless the Inspector General determines that disclosure is unavoidable during the course of the investigation. By law, Federal employees may not take or threaten to take a personnel action because of whistleblowing or the exercise of a lawful appeal, complaint, or grievance right. Non-DOI employees who report allegations may also specifically request confidentiality.