



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

U.S. DEPARTMENT OF THE INTERIOR'S ADOPTION OF CLOUD COMPUTING TECHNOLOGIES



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

MAY 21 2015

Memorandum

To: Sylvia Burns
Chief Information Officer

From: Mary L. Kendall
Deputy Inspector General

Subject: Final Evaluation Report – DOI's Adoption of Cloud-Computing Technologies
Report No. ISD-EV-OCIO-0002-2014

This report presents the results of our evaluation of the Council of the Inspectors General on Integrity and Efficiency (CIGIE) Cloud-Computing Initiative—Status of Cloud-Computing Environments within the Government. We evaluated whether selected Department of the Interior (DOI) contracts with Cloud-computing service providers incorporated best practices for mitigating key business and information technology (IT) security risks associated with moving DOI's systems and data into a public Cloud-computing environment. We also assessed the adequacy of DOI's internal controls for ensuring that only approved and secured Cloud-computing services are implemented.

We found that weaknesses in DOI's risk management and IT governance practices impeded achievement of full cloud-computing benefits and potentially placed at risk DOI's data stored in a public Cloud. We reviewed four contracts that DOI bureaus entered into with providers of Cloud-computing services. We found that none had the controls to monitor and manage their Cloud service providers and the data residing within their systems. As a result, DOI data stored in the public Cloud proved to be at risk of loss or exposure to unauthorized parties. In addition, an internal control weakness allowed the United States Geological Survey to acquire Cloud services using integrated purchase cards and to use 16 unauthorized and unsecured Cloud systems.

In our report, we make six recommendations to help DOI mitigate business and IT security risks to strengthen Cloud-computing IT governance practices. After reviewing our draft report, OCIO concurred with our recommendations. We are referring all six recommendations to the Assistant Secretary for Policy, Management and Budget to track their implementation.

The legislation creating the Office of Inspector General requires that we report to Congress semiannually on all audit, evaluation, and inspection reports issued; actions taken to implement our recommendations; and recommendations that have not been implemented. If you have any questions regarding this report, please call me at 202-208-5745.

Table of Contents

| | |
|---|----|
| Results in Brief | 1 |
| Introduction..... | 2 |
| Objective | 2 |
| Background | 2 |
| Cloud Computing | 2 |
| DOI’s Use of Public Cloud-Computing Services..... | 5 |
| Findings..... | 7 |
| DOI Practices for Acquiring and Securing Public Cloud Services Were Not Effective | 7 |
| Contracts Did Not Include Recommended Best Practices | 7 |
| DOI’s Governance of Cloud Computing Needs Strengthening..... | 11 |
| DOI Has No Accurate Inventory of its Cloud Systems..... | 11 |
| USGS Implemented Unauthorized and Unapproved Cloud Services | 11 |
| Conclusion and Recommendations..... | 14 |
| Conclusion..... | 14 |
| Recommendations Summary..... | 14 |
| Appendix 1: Scope and Methodology..... | 17 |
| Appendix 2: Response to Draft Report..... | 18 |
| Appendix 3: Status of Recommendations..... | 28 |

Results in Brief

In this evaluation of Cloud-computing technologies used by the Department of the Interior (DOI), we found that weaknesses in DOI's risk management and information technology (IT) governance practices impeded achievement of full Cloud-computing benefits and potentially placed at risk DOI's data stored in a public Cloud. A public Cloud is a shared, Internet-accessible computing environment managed by a Cloud service provider such as Amazon or Microsoft.

We reviewed four contracts that bureaus entered into with providers of Cloud-computing services. We found that none had the controls needed to monitor and manage the providers, as well as the data stored in their Cloud systems. As a result, DOI data stored in the public Cloud proved to be at risk of loss or exposure to unauthorized parties. In addition, an internal control weakness allowed the United States Geological Survey (USGS) to buy Cloud services using integrated purchase cards and to use 16 unauthorized and unsecured Cloud systems.

DOI established the Foundation Cloud Hosting Services (FCHS) indefinite delivery indefinite quantity contract in mid-2013 and mandated its use in January 2014 for all Interior public Cloud-computing acquisitions. We reviewed the contract, finding that it includes many, but not all, of the best practices mitigating risks to public Cloud-computing environments, as recommended by the Federal Chief Information Officer and Chief Acquisition Officer Councils. Also, in January 2014, DOI's chief information officer created an office to establish a Cloud-computing strategy and accelerate DOI's transition to a public Cloud-computing model for delivery of IT services. We found that the establishment of the program management office is essential for DOI oversight over the acquisition of Cloud-computing services and ensuring these services meet key IT security requirements.

As of 2014, eight DOI bureaus and three additional Federal agencies reported that they had used FCHS to purchase almost \$53 million in Cloud services. Types of services include application and web-site hosting, as well as a range of platform and infrastructure services. Moreover, DOI foresees significant increases in future Cloud usage, with up to 100 percent of new IT programs potentially beginning in the Cloud, and nearly all of DOI's current or legacy systems, as well as public data, likely to be moved to the Cloud. As DOI transitions to the Cloud, improvements to its risk management and IT governance practices are needed to safeguard data and spend IT funds effectively. We make six recommendations to DOI's chief information officer to mitigate business and IT security risks and to strengthen Cloud-computing IT governance practices.

Introduction

Objective

We evaluated whether selected DOI contracts with Cloud-computing service providers incorporated best practices for mitigating key business and IT security risks associated with moving DOI's systems and data into a public Cloud-computing environment. We also assessed the adequacy of DOI's internal controls for ensuring that only approved and secured Cloud-computing services are implemented. The scope and methodology of our review is included as Appendix 1.

Background

DOI spends about \$1 billion annually on its IT asset portfolio—systems that support a range of bureau programs that—

- protect and manage our Nation's natural resources and cultural heritage;
- provide scientific and other information to stakeholders interested in those resources; and
- help meet responsibilities to American Indians, Alaska Natives, and affiliated Island communities.

DOI's adoption of Cloud-computing technologies can improve IT service delivery and reduce the costs of managing a diverse portfolio. Specifically, Cloud computing offers DOI the potential for significant cost savings through faster application of computing resources, decreased need to buy hardware or build data centers, and increased collaboration.

Cloud Computing

The term "Cloud computing" refers to information technology systems, software, and infrastructure that a service provider packages and sells to customers. Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable, computing resources (e.g., networks, servers, storage, applications, and services). Examples of Cloud-computing systems include web-based email applications (e.g., Gmail) and other common business applications that are accessed online using a web browser. The National Institute of Standards and Technology (NIST) describes the following five essential components of Cloud systems¹:

- *On-demand self-service*: A customer can unilaterally and automatically obtain computing resources such as processing, data storage, and network bandwidth.
- *Broad network access*: Computing resources are available over the Internet or internal networks, and accessed through web browsers on a

¹NIST Special Publication (SP) 800-145, *The NIST Definition of Cloud Computing*, September 2011.

variety of devices, including smart phones, tablets, laptops, and workstations.

- *Resource pooling*: Computing resources are pooled to serve multiple customers. Resources may be assigned and reassigned according to customer demand; the customer typically has no control over or knowledge of the location of provided resources.
- *Rapid elasticity*: Resources can be allotted or reduced to align with customer needs as they go up or down. This results in computer processing, data storage, and network bandwidth that can appear unlimited to the customer.
- *Measured service*: Cloud systems automatically control and optimize resource use, based on the resources consumed. This allows resource usage to be monitored, controlled, and reported to ensure transparency for the type and amount of services used.

Cloud-computing operations generally use three service models that define an organization's control over the Cloud environment and how IT resources will be set up for use, as well as four usage models that manage the disposition of Cloud-computing resources and differentiate between classes of consumers. Specifically, NIST describes the service and usage models for Cloud systems as follows²:

Service Models

- *Infrastructure as a Service*: Capability to supply computer processing, data storage, and network bandwidth to enable the customer to use and run software, including operating systems and applications.
- *Platform as a Service*: Capability to set up on Cloud infrastructure applications created or acquired by customers using programming languages and tools supported by the provider.
- *Software as a Service*: Capability to use the provider's applications that run on Cloud infrastructure and are accessible to the client using an interface such as a web browser for e-mail.

Usage Models

- *Private Cloud*: The Cloud is operated solely for an organization; managed either by that organization or by a third party; and may exist on or off an organization's premises.
- *Public Cloud*: The Cloud remains available to the general public or to a large industry group but is owned by an organization that sells Cloud services, such as Amazon, Microsoft, or Google.
- *Community Cloud*: The Cloud is shared by several organizations; supports a specific community with a shared mission or interest; and is managed by an organization or a third party who may reside on or off the organization's premises.

²NIST Special Publication (SP) 800-145, *The NIST Definition of Cloud Computing*, September 2011.

- *Hybrid Cloud:* The Cloud is composed of two or more private, community, or public Clouds that remain unique entities but are bound together by standard or proprietary technology, which enable data and application portability.

To accelerate the Government’s use of Cloud-computing strategies, the Office of Management and Budget requires agencies to adopt a “Cloud First” policy when contemplating IT purchases. This policy also requires agencies to select secure, reliable, and cost-effective Cloud-computing alternatives when making IT investments.³ In addition, to help Federal agencies meet Cloud First requirements, the General Services Administration, in collaboration with several other agencies, established the Federal Risk Authorization Management Program (FedRAMP). FedRAMP helps agencies adopt Cloud-computing technologies by—

- ensuring that Cloud providers have adequate IT security;
- eliminating duplication of effort and reducing risk management costs; and
- enabling rapid and cost-effective purchasing of Cloud-computing services.

When transitioning to a Cloud-computing model, organizations may adopt a private Cloud strategy in which they operate their own data centers or purchase Cloud services from public providers like Amazon or Microsoft. While the private Cloud alternative enables organizations to manage their critical IT services and control access to sensitive data directly, these benefits come at the high cost of owning and operating data centers. Conversely, the public Cloud alternative frees organizations from the expense of data center ownership but requires that they effectively manage contractor performance to ensure that key business and IT security requirements are met.

According to NIST, assessing and managing risk when moving a Federal agency’s systems and data to a public Cloud poses a challenge, because the computing environment is controlled by the Cloud provider rather than the agency. Thus, effectively managing the delivery of public Cloud services requires agencies to develop contracts that address business and IT security risks, while properly defining and providing a mechanism to monitor agency and Cloud provider responsibilities. To help Federal agencies craft effective contracts with service providers the Federal Chief Information Officer and Chief Acquisition Officer Councils recommend requirements that should be included in Cloud-computing contracts to address business and IT security risks.⁴

³Office of the U.S. Federal Chief Information Officer, “25 Point Implementation Plan to Reform Federal Information Technology Management,” December 2010.

⁴ The Chief Information Officer Council is the principal interagency forum on Federal agency practices for IT management and works to improve practices related to the acquisition of Federal IT services. The Chief Acquisition Officer Council consists of acquisition professionals in the Executive branch who provide a senior level forum for monitoring and improving the Federal acquisition system through effective business practices.

Strong IT governance practices for Cloud computing help Federal agencies ensure organizational control and oversight of policies, procedures, and standards for IT service acquisition and use. The wide availability and ease of purchasing services from public Cloud providers has led to internal control problems over the acquisition of these services. For example, when Cloud-computing services are acquired without proper approvals and oversight, vulnerable systems and sensitive information may be placed in the Cloud environment; legal and privacy requirements may go unmet; and costs may quickly accrue to unacceptable levels.

DOI's Use of Public Cloud-Computing Services

DOI Secretarial Order 3309 requires that “all IT procurement expenditures, over the micropurchase level must have the approval of the Office of the Chief Information Officer (OCIO) before funds are obligated via any approved method,” which includes, among other methods, charge cards held by contracting officers⁵. Under this policy, OCIO has provided an IT strategic plan to establish a model for managing and delivering IT. Specifically, IT planning and purchasing shifts from the acquisition and management of physical IT assets (e.g., computer data centers) to the acquisition and delivery of IT as a service (e.g., Cloud-computing adoption).

Moving to this more service-oriented approach of managing and delivering IT requires fundamental organizational changes to a centralized IT management and service delivery structure, in which service providers will offer IT infrastructure, such as website hosting, desktop computing, as pre-packaged services in the Cloud. To enable the Department-wide transition to IT as a service, DOI established the Foundation Cloud Hosting Services (FCHS) contract. Examples of IT services awarded using FCHS include application and data base hosting file transfer and IT system development and testing.

We surveyed all DOI bureaus and offices to develop an inventory of implemented cloud-computing services and providers. As of 2014, eight DOI bureaus and offices had procured 42 services from 11 Cloud service providers (see Figure 1).

⁵ According to the Federal Acquisition Regulation, a micropurchase is the acquisition of goods or services using a government purchase card for an amount at or below a predefined dollar threshold. The dollar threshold varies and depends upon the type of goods or services acquired; the dollar threshold for IT services, including Cloud-computing is \$3,000

| Organization | Number of Implemented Cloud Services |
|--|--------------------------------------|
| Office of the Secretary | 2 |
| Office of Surface Mining | 2 |
| Bureau of Reclamation | 4 |
| Bureau of Safety and Environmental Enforcement | 1 |
| Bureau of Ocean and Energy Management | 2 |
| U.S. Geological Survey | 27 |
| National Park Service | 2 |
| Fish and Wildlife Service | 2 |
| | |
| Total | 42 |

Figure 1. DOI's use of Cloud-computing services as of June 2014.

Findings

DOI's adoption of Cloud-computing technologies offers the potential to significantly improve IT service delivery while reducing costs. DOI needs to improve its risk management and IT governance practices, however, to achieve these benefits. For example, we found that, on four occasions, bureaus acquired Cloud-computing services using contracts that failed to mitigate business and IT security risks inherent to public Cloud-computing environments. In addition, on 16 instances USGS acquired Cloud-computing services with integrated charge cards and then moved its data into public Clouds without approval from responsible officials and without ensuring that IT security requirements were met. These deficiencies occurred because DOI—

1. did not specify requirements that bureaus should consider when procuring Cloud-computing services and ensure those requirements were included in its contracts; or
2. fully assess and mitigate risks associated with employees using integrated charge cards to acquire Cloud-computing services.

DOI Practices for Acquiring and Securing Public Cloud Services Were Not Effective

Contracts Did Not Include Recommended Best Practices

According to NIST, assessing and managing the risks of transferring systems and data to a public Cloud poses a challenge because the Cloud provider controls the computing environment. To mitigate risks, contracts that address business and security risks unique to Cloud environments need to be developed. Specifically, contracts with Cloud service providers require clauses explaining how contractor performance will be measured, reported, and enforced, and specifying how Federal privacy, litigation discovery, and data retention and destruction requirements will be met. In addition, contracts should detail how Cloud providers perform important IT security activities (e.g., incident detection) and require that resulting IT security programs periodically be evaluated and certified by an independent third party. Finally, attention to the roles and responsibilities of the agency, the Cloud provider, and the Cloud broker also drives contractor performance, and ensures agency systems and data are adequately secured.⁶

Specifications for public Cloud services are generally called service agreements or service contracts. A service contract defines the terms and conditions for access, the use of services offered by the Cloud provider, and establishes the period of service, conditions for termination, and disposition of data (e.g., preservation period) upon contract termination. Typically, the complete terms

⁶Brokers are parties that provide services to Cloud consumers, such as enhanced security, identity management, and performance reporting, that typically are not included in the Cloud provider's service contract.

and conditions for a Cloud service contract are contained in multiple documents, including a service level agreement, as well as privacy and acceptable use policies.

NIST has identified two types of Cloud-computing service contracts—

- default nonnegotiable contracts, which are prescribed by the Cloud provider and tend not to impose requirements beyond meeting basic service and availability, do not address Federal IT security, privacy, data production, or retention and destruction requirements, and may be modified without the customer being notified; and
- negotiated contracts, which are more like traditional outsourcing contracts for IT services with terms that can be tailored to an agency’s requirements for tracking and reporting service effectiveness, and for prescribing technical controls (e.g. incident detection and handling, compliance with laws and regulations, and use of validated products meeting national or international standards, and including data ownership rights).

The Federal Chief Information Officer and Chief Acquisition Officer Councils recommend that contracts for Cloud services define performance guarantees (e.g., response time, resolution or mitigation time, and availability) and require that providers monitor their service levels, as well as report any failures to meet those levels.⁷ Contracts should include enforcement mechanisms with penalties when service levels are not met.

To determine whether DOI had implemented effective risk mitigation measures, we reviewed four major contracts used to acquire Cloud services. The contracts reviewed were Foundation Cloud Hosting Services (FCHS) and three other contracts used by Bureau of Ocean and Energy Management, Safety and Environmental Enforcement (BSEE) and USGS, respectively. In January 2014, DOI’s chief information officer mandated use of FCHS for acquiring all Cloud-computing services. Prior to the January 2014 mandate, however, many DOI bureaus had procured Cloud-computing services through other contract vehicles.

We examined whether DOI’s contracts met best practices for acquiring Cloud services recommended by the Federal Chief Information Officer and Chief Acquisition Officer Councils, as well as practices identified in FedRAMP. Specifically, we evaluated whether the contracts specified the roles and responsibilities of the parties and how contractor performance would be measured, reported, and enforced. We also assessed whether the contracts addressed Federal privacy, discovery, and data retention and destruction requirements, as well as key IT security measures (e.g., incident detection and

⁷ Chief Information Officer and Chief Acquisition Officer Councils, “Creating Effective Cloud-Computing Contracts for the Federal Government: Best Practices for Acquiring IT as a Service,” (February 2012).

handling practices), and had independent evaluation or certification of their IT security (see Figure 2).

| Contract Elements | Foundation Cloud Hosting Services Contract | USGS Contract | BSEE Contract | BOEM Contract |
|---|---|------------------------------|------------------------------|--------------------------------|
| FedRamp Approved Cloud Provider | Yes | Yes | Yes | Yes |
| Contract value and length | \$1,000,000,000 10 years | \$498,000 2 years | \$698,689 4 years | \$4,000,000 3 years |
| FIPS 199 Rating | Low, Moderate | Low | Moderate | Moderate |
| Defined roles and responsibilities of parties | Yes | Yes | No | No |
| Guaranteed system availability level | Yes | Yes | No | No |
| Reporting of service level metrics | No | No | No | No |
| Penalties for not meeting service levels | No | No | No | No |
| E-discovery requirements | Yes | No | No | No |
| Data retention and destruction policies | No | No | Yes | No |
| Data privacy requirements | Yes | No | No | No |
| Defined incident handling practices | Yes | No | No | No |
| Third party certification of IT security program | Yes | No | No | Yes |

Figure 2. Review of selected DOI use of cloud-computing contracts.

Each of the contracts we reviewed incorporated selected best practices, although none included all of the best practices. The FCHS contract met 7 out of the 10 elements, outscoring the other three contracts. For example, BOEM, and USGS contracts did not have detailed contract specifications addressing data privacy, E-

discovery, data retention, and destruction policies. They also did not have specifications defining the roles and responsibilities of the parties. Without such contract specifications to ensure protection, BOEM and USGS data in the Cloud may be at risk of unauthorized access or disclosure.

None of the contracts we reviewed specified how service provider performance would be reported, monitored, and enforced. On these contracts DOI has no way to ensure that Cloud service providers will meet required service levels, which increases the risk of mispending public funds. Finally, the BSEE, BOEM, and USGS contracts did not detail how the provider would report and respond to IT security incidents, thus increasing the risk that bureaus would be unaware if their data in the Cloud had been subject to unauthorized access, modification, or destruction. These deficiencies occurred because no single authoritative source specifies the requirements that Federal agencies should consider when procuring Cloud-computing services. Moreover, DOI did not identify requirements for bureaus procuring Cloud-computing services and ensure inclusion of those requirements in its contracts.

Recommendations

We recommend that DOI:

1. Establish specifications to be incorporated in all contracts with Cloud-computing service providers to mitigate business and IT security risks inherent to public Cloud-computing environments;
2. Modify FCHS to incorporate Federal data retention and destruction polices, including mechanism(s) to measure, report, and enforce contractor performance metrics;
3. Require that bureaus either use FCHS or a similar contract that incorporates best practices for procuring Cloud services recommended by Chief Acquisition and Chief Information Officer Councils; and
4. Migrate all existing contracts for Cloud services to FCHS or update the contract to incorporate best practices for procuring Cloud services as recommended by Chief Acquisition and Chief Information Officer Councils.

DOI's Governance of Cloud Computing Needs Strengthening

DOI Has No Accurate Inventory of its Cloud Systems

According to ISACA,⁸ having an enterprise-wide inventory of Cloud-computing services and providers is a best practice that helps organizations prevent use of unapproved or unsecured services. As of June 2014, Federal agencies are required to use only FedRAMP-approved Cloud services and providers. To comply with FedRAMP, DOI needs a complete inventory of its Cloud services and providers.

As part of our evaluation, we surveyed DOI, developing a comprehensive inventory of Cloud services and providers. We also requested that bureaus report Cloud-computing services purchased with Government integrated charge cards. As of June 2014, eight bureaus and offices had implemented 42 Cloud-computing services from 11 providers. Contracting actions procured 26 of the 42 services, with integrated charge cards used for the remaining 16. All service providers for Cloud contracts reviewed had either been approved by FedRAMP or were in the process of gaining that approval.

Bureau and DOI IT officials had an inventory of Cloud-computing services, obtained by DOI through the contracting process. Bureau and DOI IT officials were unaware, however, of the 16 public Cloud services (10 of which had been operating more than a year) acquired as micropurchases by USGS, using integrated charge cards. Over the past 5 years, USGS charged approximately \$60,000 for Amazon Cloud services on integrated charge cards. Charges ranged from a few dollars to as much as \$2,130 per month.

USGS Implemented Unauthorized and Unapproved Cloud Services

Acquiring Cloud services using integrated charge cards introduces significant IT security risks to DOI. For example, we found that DOI's system inventory did not include all 16 Cloud services and that these services operated without authorization from USGS' IT department or meeting Federal IT security requirements. Without accurate and complete inventories, DOI does not know the extent to which its data resides outside its system boundaries, subject to the risks of Cloud systems. These risks include isolation failure, interception of data in transit, and insecure or ineffective deletion of data.⁹

If exploited, these risks expose DOI's data to unauthorized parties and potentially compromise the objectives of DOI programs. Even more troubling, security

⁸ Previously known as the Information Systems Audit and Control Association, ISACA now goes by its acronym only to reflect the broad range of IT governance professionals it serves. ISACA is a global organization engaged in the development and adoption of widely accepted, industry-leading practices for information systems.

⁹ Isolation failure is the failure of the mechanisms that separate the data of different clients on the same Cloud, thus exposing sensitive data to unauthorized users. Interception of data in transit occurs when an unauthorized party uses sniffing or man-in-the-middle attacks to intercept data traveling to or from the Cloud. Insecure or ineffective deletion of data occurs when data are not truly erased from the Cloud at the end of a Cloud service contract.

controls for these 16 Cloud services were never tested to ensure controls were implemented correctly, operating as intended, and produced the desired outcome of protecting the system and its data. Moreover, the potential adverse effects to DOI were amplified because 4 of the 16 Cloud services were moderate-impact services, meaning that a breach could have a serious adverse effect on USGS assets, operations, or personnel¹⁰.

Furthermore, by using integrated charge cards to acquire Cloud services, USGS accepted the Cloud provider's default service contract, which did not include many of the recommended best practices, such as clearly defined roles and responsibilities of the parties, nor did it address Federal privacy, data production, or retention and destruction requirements. In addition, the default service contract allows the provider to unilaterally modify contract terms without notifying USGS. Being subject to the terms and conditions of the provider's default service contract puts DOI data stored in the Cloud at risk of compromise and increases the likelihood that public funds may be misspent. In response to these concerns, as of October 2014, USGS no longer authorizes the use of integrated charge cards to acquire Cloud-computing services and all USGS Cloud services that are currently purchased through the use of charge cards are to be migrated to the FCHS contract.

The internal control weakness of using integrated charge cards to acquire Cloud-computing services occurs across DOI, not just at USGS. Because we were skeptical when only one bureau in our survey reported using integrated charge cards to buy Cloud services, we took the additional step of querying DOI's financial system. We found that Bureau of Reclamation, U.S. Fish and Wildlife Service, National Park Service, and Office of the Secretary also have used integrated charge cards since January 2014 to acquire Cloud services. Specifically, from January 1, 2010 to December 31, 2014, these four bureaus and USGS charged about \$73,000 for Amazon Cloud-computing services to integrated charge cards. The deficiencies that we identified occurred because DOI did not assess and mitigate the risks of employees using their integrated charge cards to acquire public Cloud-computing services.

¹⁰According to NIST, in a moderate-impact system, the loss of confidentiality, integrity, or availability could have serious adverse effects on an organization's operations, assets, or individuals.

Recommendations

We recommend that DOI:

5. Terminate or migrate all Cloud services acquired through integrated charge cards to FCHS or a similar contract that incorporates best practices for procuring Cloud services recommended by Chief Acquisition and Chief Information Officer Councils; and
6. Prohibit use of Government micropurchase authority (e.g., Government integrated charge cards) to acquire Cloud-computing services.

Conclusion and Recommendations

Conclusion

At the time of our evaluation, eight DOI bureaus had implemented Cloud services, while others were exploring how to leverage Cloud technologies to increase operational efficiencies. DOI's move to Cloud-computing represents a paradigm shift from buying IT as a capital expenditure to buying IT as a service. Moreover, DOI has projected significant increases in Cloud usage in future years when up to 80 percent of its \$1 billion annual IT budget could be spent on Cloud-computing services. As DOI expands its use of public Cloud services, actions such as strengthening its governance and risk management practices could help mitigate the chance that a bureau's operations might be disrupted, data lost, or public funds misused. Moreover, improved coordination between DOI's chief information officer and its bureaus could ensure that unapproved and unsecured Cloud services are not implemented, and that Cloud-computing contracts incorporate best practices, while meeting all FedRAMP requirements.

Recommendations Summary

To mitigate business and IT security risks and strengthen IT governance practices pertaining to Cloud computing, we recommend that DOI:

1. Establish specifications to be incorporated in all contracts with Cloud-computing service providers to mitigate business and IT security risks inherent to public Cloud-computing environments.

OCIO response: OCIO concurred with our recommendation. OCIO stated that it will issue policy stating the requirements that must be incorporated into any contracts with cloud service providers to ensure the appropriate protections are in place to mitigate business and IT security risks.

OIG analysis: Based on the information provided, we consider this recommendation resolved, but not implemented. We will refer this recommendation to DOI's Office of Policy, Management and Budget (PMB) to track its implementation.

2. Modify FCHS to incorporate Federal data retention and destruction polices, including mechanism(s) to measure, report, and enforce contractor performance metrics.

OCIO response: OCIO concurred with our recommendation. OCIO stated that it will modify the FCHS contract to include policies for Federal data retention and destruction, performance measures and reporting, and ways the Government will enforce these requirements.

OIG analysis: Based on the information provided, we consider this recommendation resolved, but not implemented. We will refer this recommendation to PMB to track its implementation.

3. Require that bureaus either use FCHS or a similar contract that incorporates best practices for procuring Cloud services recommended by Chief Acquisition and Chief Information Officer Councils.

OCIO response: OCIO concurred with our recommendation. OCIO stated that it jointly issued with the Office of Acquisition and Property Management (PAM) a Mandatory Use Policy in January 2014 that requires all DOI organizations to use the FCHS contract for all commodity hosting services unless a waiver is approved by the chief information officer and the PAM director. Additional policy will be released, ensuring that any other contract vehicle used to acquire Cloud-computing services incorporates best practices for procuring cloud services recommended by the Federal Chief Information Officer and Chief Acquisition Officer Councils.

OIG analysis: Based on the information provided, we consider this recommendation resolved, but not implemented. We will refer this recommendation to PMB to track its implementation.

4. Migrate all existing contracts for Cloud services to FCHS or update the contract to incorporate best practices for procuring Cloud services as recommended by Chief Acquisition and Chief Information Officer Councils.

OCIO response: OCIO concurred with our recommendation. OCIO stated that it will work with all bureaus and offices to develop a plan for each of the contracts currently in place to ensure that any existing contracts for Cloud-computing services migrate to FCHS or have contract language modified to incorporate best practices for procuring such services.

OIG analysis: Based on the information provided, we consider this recommendation resolved, but not implemented. We will refer this recommendation to PMB to track its implementation.

5. Terminate or migrate all Cloud services acquired through integrated charge cards to FCHS or a similar contract that incorporates best practices for procuring Cloud services recommended by Chief Acquisition and Chief Information Officer Councils.

OCIO response: OCIO concurred with our recommendation. OCIO stated it will work with all bureaus and offices to develop a plan for all Cloud-computing services acquired through a government purchase card to be terminated or migrated to a contract that incorporates best practices

for procuring such services recommended by the Chief Acquisition and Chief Information Officer Councils.

OIG analysis: Based on the information provided, we consider this recommendation resolved, but not implemented. We will refer this recommendation to PMB to track its implementation.

6. Prohibit use of Government micropurchase authority (e.g., Government integrated charge cards) to acquire Cloud-computing services.

OCIO response: OCIO concurred with our recommendation. OCIO stated it will work with PAM to develop guidance and accompanying processes to ensure that Government purchase card use is prohibited for acquisition of Cloud-computing services.

OIG analysis: Based on the information provided, we consider this recommendation resolved, but not implemented. We will refer this recommendation to PMB to track its implementation.

Appendix I: Scope and Methodology

Scope

This evaluation, conducted as a Federal initiative managed by the Council of the Inspectors General on Integrity and Efficiency (CIGIE), focused primarily on whether Department of the Interior contracts followed best practices. We reviewed selected contract documents to determine whether they clearly defined the roles and responsibilities of the parties and the contracts' performance level in clear terms, as well as stated how performance would be measured and enforced. We also assessed whether the contracts addressed Federal privacy, E-discovery, and incident handling, as well as data retention and destruction requirements.

Information gathered during the evaluation was incorporated into a report released by CIGIE. We also looked into the cause and impact of Cloud services procured at or below the micropurchase threshold using Government integrated charge cards.

We conducted this evaluation in accordance with the Quality Standards for Inspection and Evaluation as put forth by the Council of Inspectors General on Integrity and Efficiency. We believe that the work we performed provides a reasonable basis for our conclusions and recommendations.

Methodology

To accomplish our evaluation objectives, we performed the following procedures:

- Submitted a data request to the bureaus and offices to solicit data on Cloud-computing systems used by these groups;
- Reviewed selected contract documents to substantiate the bureaus and offices' responses, then analyzed and summarized their responses;
- Interviewed applicable officials to understand the function of Office of the Chief Information Officer's Chief Management Office, the role of the Associate Director for Information Resources of U.S. Geological Survey, the role of system owners in the acquisition of the Cloud services, and the process involving Cloud services procured below the micropurchase threshold using integrated charge cards.
- Determined whether contracts with DOI's Cloud service providers incorporated practices recommended by the Chief Acquisition and Chief Information Officer Councils for mitigating risks associated with public Cloud-computing environments.

Appendix 2: Response to Draft Report

The Office of the Chief Information Officer's response to our draft report follows on page 19.




United States Department of the Interior

OFFICE OF THE SECRETARY
Washington, DC 20240

APR 23 2015

To: Kimberly Elmore
Assistant Inspector General for Audits, Inspections, and Evaluations

From: Sylvia Burns
Chief Information Officer 

Subject: Office of Inspector General, Draft Evaluation Report
U.S. Department of the Interior's Adoption of Cloud Computing Technologies,
Report No. ISDN-EV-OCI-0002-2014

The Department of the Interior (DOI), Office of the Chief Information Officer (OCIO), appreciates the opportunity to review Office of Inspector General (OIG) draft Evaluation Report, DOI's Adoption of Cloud Computing Technologies, Report No. ISDN-EV-OCI-0002-2014. In response to this report and as required, Attachment 1 provides a Statement of Actions planned by DOI to implement OIG's recommendations, the responsible officials, and the target dates for implementation. Attachments 2 and 3 are responses provided by U.S. Geological Survey (USGS) and Bureau of Safety and Environmental Enforcement/Bureau of Ocean and Energy Management (BSEE/BOEM) respectively, to address findings identified in the draft Report.

If you have any questions, please contact me at (202) 208-6194. Staff may contact Steven B. Thompson, Acting Director, Internal Control, Audit, and Compliance Management (ICACM) at (202) 821-8887.

cc: Alexandra Lampros, Financial Specialist, Office of Financial Management
Steven B. Thompson, Acting Director, Internal Control, Audit, and Compliance Management

Attachments:

1. OCIO Statement of Actions to Address Office of Inspector General Draft Evaluation Report U.S. Department of the Interior's Adoption of Cloud Computing Technologies Report No. ISDN-EV-OCI-0002-2014
2. USGS Response to Findings Identified in the Office of Inspector General Draft Evaluation Report, U.S. Department of the Interior's Adoption of Cloud-Computing Technologies Report No. ISDN-EV-OCI-0002-2014
3. BSEE/BOEM Response to Findings Identified in the Office of Inspector General Draft Evaluation Report, U.S. Department of the Interior's Adoption of Cloud-Computing Technologies Report No. ISDN-EV-OCI-0002-2014

Attachment 1

Office of the Chief Information Officer
Statement of Actions to Address Office of Inspector General Draft Evaluation Report
U.S. Department of the Interior's Adoption of Cloud Computing Technologies
Report No. ISDN-EV-OCI-0002-2014

Recommendations – To mitigate business and information technology (IT) security risks and strengthen IT governance practices pertaining to Cloud computing, we recommend that Department of the Interior (DOI):

Recommendation 1: *Establish specifications to be incorporated in all contracts with Cloud-computing service providers to mitigate business and IT security risks inherent to public Cloud-computing environments.*

Response: The DOI Office of the Chief Information Officer (OCIO) concurs with the finding and accompanying recommendation. The OCIO will issue policy stating the requirements that must be incorporated into any contracts with cloud service providers (CSPs) to ensure that the appropriate protections are in place to mitigate business and IT security risks.

Responsible Official & Title: Maria Clark, Chief Management Officer (CMO), Office of the Chief Information Officer (OCIO)

Lead Contact & Title: Peggy-Lee O'Connor, Hosting Customer Relationship Management Chief, Chief Management Office (CMO), Office of the Chief Information Officer (OCIO)

Target Completion Date: June 30, 2015

Recommendation 2: *Modify FCCHS to incorporate Federal data retention and destruction policies, including mechanism(s) to measure, report, and enforce contractor performance metrics.*

Response: The DOI OCIO concurs with the finding and accompanying recommendation. The OCIO, working with the Foundation Cloud Hosting Services Contract Contracting Officer (CO), will modify the 10 Indefinite Delivery/Indefinite Quantity (ID/IQ) Contracts to include the following language:

"Individual Task Orders awarded through the Foundation Cloud Hosting Services Contract will address Federal data retention and destruction requirements as necessary to comply with individual Agency/Bureau requirements. Further, performance measures, reporting requirements, and how the government will enforce those requirements will be defined and stated in the individual task orders. This clause shall flow down to any/all subcontractors at the Task Order level."

Responsible Official & Title: Maria Clark, Chief Management Officer (CMO), Office of the Chief Information Officer (OCIO)

Lead Contact & Title: Peggy-Lee O'Connor, Hosting Customer Relationship Management Chief, Chief Management Office (CMO), Office of the Chief Information Officer (OCIO)

Target Completion Date: April 30, 2015

Recommendation 3: *Require that bureaus either use FCHS or a similar contract that incorporates best practices for procuring Cloud services recommended by Chief Acquisition and Chief Information Officer Councils.*

Response: The DOI OCIO concurs with the finding and accompanying recommendation. The OCIO along with the Office of Acquisition and Property Management (PAM), jointly issued a Mandatory Use Policy in January 2014 that requires all DOI subcomponent organizations to utilize the Foundation Cloud Hosting Services Contract for all commodity hosting services unless a waiver is approved by the CIO and the Director, PAM. Additional policy will be released (see Recommendation 1 above) ensuring that any other contract vehicle utilized to acquire cloud computing services incorporates best practices for procuring cloud services recommended by the Chief Acquisition and Chief Information Officer Councils.

Responsible Official & Title: Maria Clark, Chief Management Officer (CMO), Office of the Chief Information Officer (OCIO)

Lead Contact & Title: Peggy-Lee O'Connor, Hosting Customer Relationship Management Chief, Chief Management Office (CMO), Office of the Chief Information Officer (OCIO)

Target Completion Date: June 30, 2015

Recommendation 4: *Migrate all existing contracts for Cloud services to FCHS or update the contract to incorporate best practices for procuring Cloud services as recommended by Chief Acquisition and Chief Information Officer Councils.*

Response: The DOI OCIO concurs with the finding and accompanying recommendation. The OCIO will work with all bureaus and offices to develop a plan (depending on the period of performance of existing cloud service contracts) for each of the contracts currently in place to ensure that any existing contracts for cloud services migrate to the FCHS or have contract language modified to incorporate best practices for procuring cloud services.

Responsible Official & Title: Maria Clark, Chief Management Officer (CMO), Office of the Chief Information Officer (OCIO)

Lead Contact & Title: Peggy-Lee O'Connor, Hosting Customer Relationship Management Chief, Chief Management Office (CMO), Office of the Chief Information Officer (OCIO)

Target Completion Date: December 31, 2015

Target Completion Date: December 31, 2015

Recommendation 5: *Terminate or migrate all Cloud services acquired through integrated charge cards to FCHS or a similar contract that incorporates best practices for procuring Cloud services recommended by Chief Acquisition and Chief Information Officer Councils.*

Response: The DOI OCIO concurs with the finding and accompanying recommendation. The OCIO will work with all bureaus and offices to develop a plan for all cloud services acquired through a government purchase card are terminated or migrated to a cloud contract that incorporates best practices for procuring cloud services recommended by the Chief Acquisition and Chief Information Officer Councils.

Responsible Official & Title: Maria Clark, Chief Management Officer (CMO), Office of the Chief Information Officer (OCIO)

Lead Contact & Title: Peggy-Lee O'Connor, Hosting Customer Relationship Management Chief, Chief Management Office (CMO), Office of the Chief Information Officer (OCIO)

Target Completion Date: December 31, 2015

Recommendation 6: *Prohibit use of Government micropurchase authority (e.g., Government integrated charge cards) to acquire Cloud-computing services.*

Response: The Department of the Interior (DOI) Office of the Chief Information Officer (OCIO) concurs with the finding and accompanying recommendation. OCIO will work with the PAM to develop guidance/policy and accompanying processes to ensure that the use of government purchase cards is prohibited in the acquisition of cloud-computing services.

Responsible Official & Title: Maria Clark, Chief Management Officer (CMO), Office of the Chief Information Officer (OCIO)

Lead Contact & Title: Peggy-Lee O'Connor, Hosting Customer Relationship Management Chief, Chief Management Office (CMO), Office of the Chief Information Officer (OCIO)

Target Completion Date: December 31, 2015

Attachment 2

USGS Response to Findings Identified in the Office of Inspector General Draft Evaluation Report, U.S. Department of the Interior's Adoption of Cloud-Computing Technologies Report No. ISDN-EV-OCI-0002-2014

Recommendation 4: *Migrate all existing contracts for Cloud services to FCHS or update the contract to incorporate best practices for procuring Cloud services as recommended by Chief Acquisition and Chief Information Officer Councils.*

Response: The United States Geological Survey (USGS) concurs with the finding and accompanying recommendation. The USGS cloud contract that was reviewed and reported in ISDN-EV-OCI-0002-2014 was modified in February 2015 to incorporate best practices for procuring cloud services recommended by Chief Acquisition and Chief Information Officer Councils, including data privacy, E-Discovery, data retention, destruction policies, roles and responsibilities, provider performance and incident response. USGS is also working with OCIO in migrating current cloud applications to the cloud both through the USGS contract that was modified or through the FCHS contract.

Responsible Official & Title: Joe Seger, Deputy Chief, Office of Enterprise Information, U.S. Geological Survey (USGS)

Lead Contact & Title: Alan Wiser, Chief Information Security Officer, Office of Enterprise Information, U.S. Geological Survey (USGS)

Target Completion Date: December 31, 2015

Recommendation 5: *Terminate or migrate all Cloud services acquired through integrated charge cards to FCHS or a similar contract that incorporates best practices for procuring Cloud services recommended by Chief Acquisition and Chief Information Officer Councils.*

Response: The United States Geological Survey (USGS) concurs with the finding and accompanying recommendation. In October 2014, the USGS Acting Director, issued a memo, "Cloud Computing Services Compliance Guidance" to all USGS employees, contractors and volunteers and emeriti. This memo states, "Effective immediately, cloud computing services are not authorized for purchase using a Government charge card." The memo also states that current cloud services purchased through use of charges cards are to be migrated to FCHS or a similar contract. Additionally, the USGS developed a process to ensure that USGS / DOI information and applications are not placed into unauthorized and unsecured cloud services as documented through Plan of Action and Milestones (POA&M) 27992. This process is described in the "Process to ensure USGS Cloud services meets FedRAMP security requirements" document, and is being followed in migrating services from charge cards to appropriate contracts. All USGS memos and guidance concerning cloud security requirements are internally available to all USGS staff and referenced in our cloud procurement procedures.

Responsible Official & Title: Joe Seger, Deputy Chief, Office of Enterprise Information, U.S. Geological Survey (USGS)

Lead Contact & Title: Alan Wiser, Chief Information Security Officer, Office of Enterprise Information, U.S. Geological Survey (USGS)

Target Completion Date: December 31, 2015

Recommendation 6: *Prohibit use of Government micro-purchase authority (e.g., Government integrated charge cards) to acquire Cloud-computing services.*

Response: The United States Geological Survey (USGS) concurs with the finding and accompanying recommendation. In October 2014, the USGS Acting Director, issued a memo, "Cloud Computing Services Compliance Guidance" to all USGS employees, contractors and volunteers and emeriti. This memo states, "Effective immediately, cloud computing services are not authorized for purchase using a Government charge card." The memo also states that current cloud services purchased through use of charges cards are to be migrated to FCHS or a similar contract. Additionally, the USGS developed a process to ensure that USGS / DOI information and applications are not placed into unauthorized and unsecured cloud services as documented through Plan of Action and Milestones (POA&M) 27992. This process is described in the "Process to ensure USGS Cloud services meets FedRAMP security requirements" document, and is being followed in migrating services from charge cards to appropriate contracts. All USGS memos and guidance concerning cloud security requirements are internally available to all USGS staff and referenced in our cloud procurement procedures.

Responsible Official & Title: Joe Seger, Deputy Chief, Office of Enterprise Information, U.S. Geological Survey (USGS)

Lead Contact & Title: Alan Wiser, Chief Information Security Officer, Office of Enterprise Information, U.S. Geological Survey (USGS)

Target Completion Date: December 31, 2015

Attachment 3

BSEE/BOEM Response to Findings Identified in the Office of Inspector General Draft Evaluation Report, U.S. Department of the Interior's Adoption of Cloud-Computing Technologies Report No. ISDN-EV-OCI-0002-2014

On October 22, 2014, the BSEE Technology Services Division received *Notifications of Potential Findings and Recommendations*, which suggested that BOEM and BSEE contracts do not include all of the best practices for acquiring cloud services, as recommended by the Federal Chief Information Officer and the Chief Acquisition Officers Council. BSEE / BOEM appreciated the opportunity to review the potential findings and concurred that there were opportunities for improvement. On November 5, 2014, BSEE / BOEM provided the OIG with details that contradicted some of their potential findings, and respectfully asked that the OIG clarify their findings accordingly. BSEE / BOEM would like to have the opportunity to meet with the OIG to review the re-evaluation that was performed and also be provided more details to ensure that follow-up actions / recommendations can be completed as required.

Moving forward, we plan to achieve a greater level of compliance with known best practices for acquiring cloud services. Specifically, the following initiatives are underway to address the OIG recommendations, as they relate to the in-scope contracts for BOEM (Simultaneous Ascending Clock Auction system) and BSEE (ServiceNow)*.

Recommendation 1: *Establish specifications to be incorporated in all contracts with Cloud-computing service providers to mitigate business and IT security risks inherent to public Cloud-computing environments.*

Response: BOEM / BSEE concurs with the finding and accompanying recommendation. BOEM / BSEE will follow any policy issued by the OCIO stating the requirements that must be incorporated into any contracts with cloud service providers (CSPs) to ensure that the appropriate protections are in place to mitigate business and IT security risks.

Responsible Official & Title: Thomas Hoyler, Chief Information Security Officer, BOEM/BSEE

Lead Contact & Title: Thomas Hoyler, Chief Information Security Officer, BOEM/BSEE

Target Completion Date: June 30, 2015

Recommendation 2: *Modify FCHS to incorporate Federal data retention and destruction policies, including mechanism(s) to measure, report, and enforce contractor performance metrics.*

Response: BSEE / BOEM concurs with the finding and accompanying recommendation. BSEE / BOEM will ensure that any task orders awarded through the FCHS contract will contain the appropriate language and/or specific performance metrics required for each requirement awarded to support any BSEE / BOEM cloud enabled service / application.

Responsible Official & Title: Thomas Hoyler, Chief Information Security Officer, BOEM/BSEE

Lead Contact & Title: Thomas Hoyler, Chief Information Security Officer, BOEM/BSEE

Target Completion Date: April 30, 2015

Recommendation 3: *Require that bureaus either use FCHS or a similar contract that incorporates best practices for procuring Cloud services recommended by Chief Acquisition and Chief Information Officer Councils.*

Response: BSEE / BOEM concurs with the finding and accompanying recommendation. OCIO along with the Office of Acquisition and Property Management (PAM) jointly issued a Mandatory Use Policy in January 2014 that requires all DOI subcomponent organizations to utilize the Foundation Cloud Hosting Services Contract for all commodity hosting services unless a waiver is approved by the CIO and the Director, PAM. No action by BSEE / BOEM at this time as bureaus are abiding by the policy issued and is currently moving forward with several cloud requirements, working with the OCIO and the FCHS Hosting PMO team.

Responsible Official & Title: Thomas Hoyler, Chief Information Security Officer, BOEM/BSEE

Lead Contact & Title: Thomas Hoyler, Chief Information Security Officer, BOEM/BSEE

Target Completion Date: Completed

Recommendation 4: *Migrate all existing contracts for Cloud services to FCHS or update the contract to incorporate best practices for procuring Cloud services as recommended by Chief Acquisition and Chief Information Officer Councils.*

Response: BSEE / BOEM concurs with the finding and accompanying recommendation. BOEM is currently migrating the Simultaneous Ascending Clock Auction System (Wind Auction Services) to the DOI FCHS contract under RFQ #D15PS00164 (quotes are due no later than 2:00 p.m. ET on Friday, April 10, 2015). In addition, BSEE expects to migrate the ServiceNow contract to the DOI FCHS contract at the expiration of the final option year. BSEE will exercise the final option year in July. It should be noted that both of these contracts were awarded well before the existence of the DOI FCHS contract, and both were approved via the DOI OCIO Spending Plan Portal.

Responsible Official & Title: Thomas Hoyler, Chief Information Security Officer, BOEM/BSEE

Lead Contact & Title: Thomas Hoyler, Chief Information Security Officer, BOEM/BSEE

Target Completion Date: July 30, 2016

Recommendation 5: *Terminate or migrate all Cloud services acquired through integrated charge cards to FCHS or a similar contract that incorporates best practices for procuring Cloud services recommended by Chief Acquisition and Chief Information Officer Councils.*

Response: At this time BSEE / BOEM does not have any cloud services that have been acquired through government purchase cards. No action is required by BSEE / BOEM.

Responsible Official & Title: Thomas Hoyler, Chief Information Security Officer, BOEM/BSEE

Lead Contact & Title: Thomas Hoyler, Chief Information Security Officer, BOEM/BSEE

Target Completion Date: Completed

Recommendation 6: *Prohibit use of Government micro-purchase authority (e.g., Government integrated charge cards) to acquire Cloud-computing services.*

Response: BSEE / BOEM concurs with the finding and accompanying recommendation. Once OCIO / PAM issue policy related to the use of government purchase cards, BSEE / BOEM will ensure that the policy is distributed and any follow up actions are completed.

Responsible Official & Title: Thomas Hoyler, Chief Information Security Officer, BOEM/BSEE

Lead Contact & Title: Thomas Hoyler, Chief Information Security Officer, BOEM/BSEE

Target Completion Date: December 31, 2015

*Note: The BOEM EcoSpatial Information Database (ESID) was also referenced in Figure 1 within the Evaluation Report; however, that system was not formally evaluated (presumably because it is a FIPS 199 Low Impact System)

Appendix 3: Status of Recommendations

| Recommendations | Status | Action Required |
|-----------------|------------------------------|---|
| 1 - 6 | Resolved but not implemented | We will refer these recommendations to PMB to track their implementation. |

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.doi.gov/oig/index.cfm

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