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

The U.S. Department of the Interior Needs To Better Protect Data Stored in the Cloud From the Risk of Unauthorized Access

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

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

FEB 21 2024

Memorandum

To: Darren Ash
Chief Information Officer

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

Subject: Final Evaluation Report – *The U.S. Department of the Interior Needs To Better Protect Data Stored in the Cloud From the Risk of Unauthorized Access*
Report No. 2022-ITA-025

This memorandum transmits our evaluation report on the U.S. Department of the Interior's (Department's) cloud-computing controls to prevent the loss of sensitive data hosted by cloud service providers (CSPs). Specifically, we determined whether sensitive, personally identifiable information hosted by CSPs are at risk of unauthorized access. We also assessed the Department's internal controls for contractor oversight, to include detecting and preventing deployment of unapproved and unauthorized cloud services. Finally, we reviewed whether select Department contracts with CSPs included recommended best practices for mitigating key business and IT security risks associated with moving Department systems and data into a cloud environment.

We will track open recommendations for resolution and implementation. We will notify Congress about our findings, and we will report semiannually, as required by law, on actions you have taken to implement the recommendations and on recommendations that have not been implemented. We will also post a public version of this report on our website.

If you have any questions about this report, please contact me at aie_reports@doioig.gov.

cc: June Hartley, Deputy Chief Information Officer
Stanley Lowe, Chief Information Security Officer

Contents

Report Abbreviations

Abbreviation	Definition
ACIO	Associate Chief Information Officer
APT	Advanced Persistent Threat
CAO	Chief Acquisition Officer(s)
CIO	Chief Information Officer(s)
CSAM	Cyber Security Assessment and Management
CSP	Cloud Service Provider
CUI	Controlled Unclassified Information
Department	U.S. Department of the Interior
DLP	Data Loss Prevention
FCHS	Foundation Cloud Hosting Services
FedRAMP	Federal Risk and Authorization Management Program
FISMA	Federal Information Security Modernization Act
GRC	Governance, Risk, and Compliance
IT	Information Technology
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OMB	U.S. Office of Management and Budget
PAM	Office of Acquisition and Property Management
PII	Personally Identifiable Information
SP	Special Publication
TIC	Trusted Internet Connection
USGS	U.S. Geological Survey

Results in Brief

What We Evaluated

Adopting cloud technologies can potentially improve information technology (IT) service delivery and reduce the costs of managing the U.S. Department of the Interior's (Department's) diverse portfolio. Since 2010, the U.S. Office of Management and Budget has adopted strategies to accelerate the Federal Government's use of cloud-computing services. Using cloud-computing services, however, introduces business and cybersecurity risks that must be mitigated.

Recognizing the inherent risks associated with cloud computing and the degree to which Federal agencies overall and the Department in particular have increased their adoption and use of cloud services, we first evaluated the Department's adoption of cloud computing in 2015. We identified weaknesses in the Department's risk management and IT governance practices that impeded achievement of full cloud-computing benefits and potentially placed the Department's cloud-stored data at risk.[1]

The objective of our current evaluation was to determine whether the Department's cloud-computing security controls are effective in preventing the loss of sensitive Department data transmitted, processed, and stored by cloud service providers (CSPs). To accomplish this, we examined security controls for a Department CSP that contains sensitive personally identifiable information (PII).[2] We also assessed the Department's internal controls for contractor oversight, including assessment detecting and preventing deployment of unauthorized cloud services. Finally, we reviewed whether selected Department contracts with CSPs complied with Department policies and included recommended best practices for mitigating key business and IT security risks associated with moving Department systems and data into a cloud.

What We Found

While we found that the Department has improved its acquisition and implementation of cloud-computing services since our 2015 evaluation, we also found that weaknesses in the Department's cyber risk management and contractor oversight practices put sensitive PII for tens of thousands of Federal employees at risk of unauthorized access. As part of a weeklong exercise, we emulated a sophisticated adversary attempting to exfiltrate (steal) sensitive data from a Department system, which is hosted in a cloud. Using the same techniques as malicious actors, we successfully exfiltrated over a gigabyte of fictitious sensitive PII[3] from the system.

[1] *The U.S. Department of the Interior's Adoption of Cloud Computing Technologies* (Report No. ISDN–EV–OCI–0002–2014), issued May 2015.

[2] The National Institute of Standards and Technology (NIST) defines PII as information that can be used to distinguish or trace an individual's identity—such as name, social security number, biometric data records—either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual (e.g., date and place of birth, mother's maiden name, etc.).

[3] To protect identities while simulating malicious actors exfiltrating data, we used realistic, privacy-law-compliant test data.

As we conducted more than 100 tests, we monitored the Department's computer logs and incident tracking system in real time. Over the course of the week, none of these tests were prevented by the Department's data loss prevention (DLP) solution or recognized as malicious activity by Department IT security analysts.[4] Our tests succeeded because the Department failed to implement security measures capable of either preventing or detecting well-known and widely used techniques employed by malicious actors to steal sensitive data. Moreover, in the years that the system has been hosted in a cloud, the Department has never conducted regular required tests of the system's controls for protecting sensitive data from unauthorized access. Moreover, the system is designated as a high-value asset[5]; consequently, the loss or corruption of sensitive data or loss of access to the system would have serious impacts on the Department's ability to perform its mission or conduct business. As the system contains PII on many people, a breach could harm Department operations and could potentially cost the Department millions of dollars to provide credit-monitoring services for the individuals whose personal information was part of the PII breach.

We also found that deficiencies in the Department's governance practices resulted in the acquisition and deployment of cloud services from unapproved CSPs. As a result, the Department did not have a complete inventory of its cloud systems or assurance that the cloud services met Federal requirements. Finally, we found that the Department can improve oversight of its CSPs both by enforcing penalties when CSPs fail to meet contractually required service levels and ensuring that contracts with CSPs incorporate required Office of the Chief Information Officer (OCIO) standards and best practices for procuring cloud services.

Why This Matters

The March 2023 *National Cybersecurity Strategy* states, "Malicious cyber actors exploit U.S.-based cloud infrastructure . . . to carry out criminal activity, malign influence operations, and espionage against individual victims, businesses, governments, and other organizations in the Unites States and abroad."[6] According to various media publications, in July 2023, a major software company reported that a Chinese advanced persistent threat[7] (APT) group with espionage objectives against Western governments exploited security control weaknesses to steal a cryptographic key from the company's computer systems. It was reported that the key allowed the hackers to gain unauthorized access to cloud-based email systems for 25 organizations, including the U.S. Departments of Commerce and State. According to a public report, the

[4] Data loss prevention capabilities identify, detect, and prevent sensitive information from leaving an organization. https://csrc.nist.gov/glossary/term/data_loss_prevention.

[5] OCIO information system security documentation indicates that the subject system is a high-value asset.

[6] The White House, *National Cybersecurity Strategy*, issued March 2023, https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

[7] An advance persistent threat (APT) is a well-resourced adversary engaged in sophisticated malicious cyber activity that is targeted and aimed at prolonged network/system intrusion. APT objectives could include espionage, data theft, and network/system disruption or destruction. https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats-and-nation-state-actors.

hackers gained access to the Commerce Secretary's email account and exfiltrated 60,000 unclassified emails from 10 Department of State employees.[8]

Although we do not suggest that the Department of the Interior faces the same types of risk as those set forth in the press coverage regarding this incident, this recent attack by an apparent nation-state cyber actor illustrates the importance of having a robust DLP capability to protect sensitive data from unauthorized access. As the reported breach of a major CSP shows, it may be impossible to prevent a well-resourced adversary from compromising an organization's computer systems; however, an effective DLP capability may prevent the adversary from exfiltrating the organization's data.

Operating in the cloud without meeting key IT security requirements potentially puts Department systems—and the sensitive information and PII they contain—at increased risk of compromise. According to the National Institute of Standards and Technology, assessing and managing the risks of transferring systems and data to a cloud poses a challenge because the computing environment is under the control of the cloud provider. These risks include isolation failure, interception of data in transit, and insecure or ineffective deletion of data.[9] Effectively managing the delivery of cloud services requires agencies to develop contracts that address business and IT security risks. Accordingly, the Department must implement a strong IT governance process to ensure CSPs hosting Department systems and data meet all Federal and departmental security requirements.

What We Recommend

We make 10 recommendations to help strengthen the Department's cyber risk management, contractor oversight, and IT governance practices for its cloud services.

[8] Demirjian, Karoun. "Chinese Hackers Stole 60,000 State Dept. Emails in Breach Reported in July," *New York Times*, September 27, 2023.

[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 erased from the cloud at the end of a cloud service contract.

Introduction

Objective

We evaluated whether the U.S. Department of the Interior's (Department's) cloud-computing security controls prevent the loss of sensitive Department data hosted by cloud service providers (CSPs). As part of our evaluation, we also assessed the Department's internal controls for detecting and preventing the acquisition and deployment of unapproved and unauthorized cloud services. Finally, we evaluated whether selected Department contracts with CSPs incorporated recommended best practices for mitigating key business and IT security risks associated with moving Department systems and data into a cloud-computing environment.

See Appendix 1 for the scope and methodology of our review.

Background

In fiscal year 2022, the Department spent approximately $1.6 billion on its IT asset portfolio[10] of systems that support a range of bureau programs, including those that:

- Protect and manage our natural resources and cultural heritage.
- Provide scientific and other information to stakeholders interested in those resources.
- Help meet responsibilities to American Indians, Alaska Natives, and affiliated Island Communities.

The Department's IT asset portfolio includes over 100 cloud-based systems hosted by dozens of CSPs. In fiscal year 2022, the Department spent $233 million on cloud-computing services—approximately 15 percent of its total IT spending that year.

Cloud Computing

The term "cloud computing" refers to IT systems, software, and infrastructure that a CSP packages and sells to customers. In particular, 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 and other common business applications that are accessed online using a web browser.

[10] IT spending information obtained from https://www.itdashboard.gov, an official website of the U.S. Government.

The National Institute of Standards and Technology (NIST) describes the following five essential characteristics of cloud systems[11]:

- *On-demand self-service*. A customer can unilaterally and automatically obtain computing resources, such as processing, data storage, and network bandwidth without human interaction with each service provider.

- *Broad network access*. Computing resources are available over the internet or internal networks and accessed through web browsers on a variety of devices, including mobile 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. 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 the customer to ensure transparency for the type and number of services used.

The adoption of cloud technologies has the potential to improve IT service delivery and reduce the costs of managing an organization's diverse IT portfolio. For the Federal Government in particular, cloud computing offers the potential for significant cost savings through increased collaboration and faster provisioning of computing resources, which also decreases the need to buy hardware or build data centers.

Federal Government Adoption of Cloud-Computing Services

In December 2010, to accelerate the Federal Government's use of cloud-computing strategies, the U.S. Office of Management and Budget (OMB) required agencies to adopt a "Cloud First" policy when contemplating IT purchases and evaluate secure, reliable, and cost-effective cloud-computing alternatives when making new IT investments.[12] Subsequently, in June 2019, the Federal Chief Information Officer (CIO) introduced "Cloud Smart" to replace "Cloud First" as a long-term, high-level strategy to drive cloud adoption in Federal agencies. This new strategy supported agencies in efforts to achieve additional savings and security and deliver faster services.[13]

[11] NIST Special Publication (SP) 800–145, *The NIST Definition of Cloud Computing*, September 2011.

[12] Office of the Federal Chief Information Officer, *25 Point Implementation Plan to Reform Federal Information Technology Management*, issued December 2010.

[13] Office of the Federal Chief Information Officer, *Federal Cloud Computing Strategy*, issued June 2019.

The General Services Administration, in collaboration with several other agencies, established the Federal Risk and Authorization Management Program (FedRAMP) in 2011 to accelerate the adoption of cloud-computing services by Federal agencies. Specifically, FedRAMP helps agencies adopt cloud-computing technologies by:

- Ensuring cloud providers have adequate IT security.
- Eliminating duplication of effort and reducing risk management costs.
- Enabling rapid, cost-effective purchasing of cloud-computing services.

Since December 2011, the OMB has required Federal agencies to obtain cloud services that are certified under FedRAMP. Specifically, to be FedRAMP certified at the time of our current evaluation, the CSP was required to meet the security control requirements from NIST SP 800–53, Revision 4, security control baselines and to have an independent third-party security control assessment.[14] FedRAMP requirements for cloud-computing services help ensure the integrity and security of agency data that is transferred, processed, or stored in cloud environments. Because CSPs often offer a mix of cloud-based services, some of which are FedRAMP compliant and some of which are not, Federal agencies must use caution to ensure that they are acquiring only FedRAMP complaint services.

Cloud-Computing Risks

As noted previously, the use of cloud-computing services introduces business and cybersecurity risks that must be mitigated. According to the NIST, assessing and managing the risks of transferring systems and data to a cloud pose a challenge because the computing environment is under the control of the cloud provider.[15] Thus, effectively managing the delivery of cloud services requires agencies to develop contracts that address both business and IT security risks. Moreover, 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 CSPs can lead to internal control problems concerning 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 not be addressed, and costs may quickly increase to unacceptable levels.

In cloud-based systems, the CSP and the agency share responsibility for implementing required security controls. For example, because the CSP physically hosts the cloud system, the CSP is responsible for implementing the NIST-required physical and environmental security controls, while the agency is responsible for implementing the access controls for system users. The Federal agency's system security plan[16] documents the controls implemented in the system

[14] NIST SP 800–53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013.

[15] NIST SP 800–144, *Guidelines for Security and Privacy in Public Cloud Computing,* December 2011.

[16] According to NIST's *Guide for Developing Security Plans for Federal Information Systems* (NIST SP 800–18, Revision 1, February 2006), a system security plan is a "formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements."

as well as the party responsible for implementing and monitoring these controls. Controls related to securing sensitive data from unauthorized access (e.g., data loss prevention (DLP) controls that capture and monitor network traffic in real time and identify sensitive data) as well as detecting and responding to IT security incidents may be the responsibility of the agency or the CSP, depending on the system security plan.

Once cloud-computing services are acquired, agencies must ensure that all approved and authorized information systems are properly identified and accounted for. Federal guidance specifically requires agencies to maintain an accurate inventory of these systems. To help ensure cloud-based systems are included in that system inventory, the OMB provides guidance on developing system inventories and associated reporting requirements.[17] An "enterprise-wide information system inventory" is a complete inventory of agency information resources, including personnel, equipment, and funds devoted to information resources management and information technology, with an appropriate level of detail. Adherence to these standards helps ensure that the systems and the information processed, communicated, or stored by those systems can be properly secured to protect the confidentiality, integrity, and availability of data resident in agency information systems and cloud-computing services.

The Department's Use of Cloud-Computing Services

The Department's Office of the Chief Information Officer (OCIO) is responsible for developing and overseeing Departmentwide risk-based, cost-effective policies and procedures for addressing information security. To mitigate business and IT security risks associated with cloud computing, the OCIO established the Cloud Program Office, which reports to the OCIO and is responsible for providing support for customers looking to acquire cloud-based services for their organization using the Foundation Cloud Hosting Services (FCHS) contracts and other available services. The FCHS contracts help to define and architect IT solutions that take full advantage of cloud-computing scalability and elasticity so that cloud-computing capabilities can be rapidly provisioned and expanded to meet existing and future mission needs.

In January 2014, the Cloud Program Office mandated FCHS contract use for all Department cloud-computing acquisitions unless the bureau or office receives a waiver from the Cloud Program Office to procure cloud services using micropurchase authority.[18] Further, on September 24, 2020, to help ensure that all Department cloud services are FedRAMP approved and appropriate security mitigations are in place, the OCIO issued an announcement requiring bureaus and offices to use the following process when obtaining cloud services:

1. Review the Department CSPs and catalog and select a pre-approved enterprise offering contract that meets business requirements.

2. Use the FCHS contracts if business requirements cannot be met by an existing service or task order.

[17] OMB Circular No. A–130, *Managing Information as a Strategic Resource*, issued July 2016.

[18] The Department issued a memorandum, *Mandatory Use Policy for the Department of the Interior Foundation Cloud Hosting Services Contract*, on January 6, 2014.

3. Request a waiver to the mandatory use policy if FCHS contracts do not satisfy business requirements.

The Department currently has 49 approved CSPs to support delivery of cloud-based IT services throughout the Federal Government. All cloud procurements, including those that are issued against one of the approved enterprisewide cloud hosting solutions, must be approved by the bureau or office Associate Chief Information Officer (ACIO).[19] ACIOs are responsible for ensuring that their respective bureau or office does not have cloud procurements that are inappropriately acquired outside of this process.

Prior Cloud-Computing Evaluation Coverage

In 2015, we performed an evaluation of the Department's cloud-computing program. During this review, we identified weaknesses in Department's risk management and IT governance practices that impeded achievement of full cloud-computing benefits and potentially placed the Department's cloud-stored data at risk of unauthorized access or disclosure.

Specifically, we reviewed four contracts that Department bureaus entered with providers of cloud-computing services. We found that none had the controls to monitor and manage their CSPs and the data residing within their systems. As a result, Department data stored in the public cloud was at risk of loss or exposure to unauthorized parties. In addition, an internal control weakness allowed the U.S. Geological Survey (USGS) to acquire 16 cloud services using integrated purchase cards. Acquiring cloud services in this way introduces significant IT security risks to the Department because of the lack of centralized controls over such purchases. For example, we found that Department's information system inventory did not include any of the 16 USGS cloud services and that these services operated without having authorization from USGS' IT department or meeting Federal IT security requirements.

In our report, we made six recommendations to help the Department mitigate business and IT security risks to strengthen cloud-computing IT governance practices. These recommendations were closed based on information received at that time. However, during our current review, we determined that the corrective action steps previously taken by the Department do not appear to have fully addressed some of the findings that we previously identified. As a result, we have included two new findings that, to some extent, reiterate conclusions in our earlier report.

Appendix 2 summarizes the earlier recommendations and our assessment of their status now.

[19] Department memorandum, *Acquisition of Information Technology Cloud Services/Mandatory Use of Pre-Approved Cloud Hosting Services and Contracts*, issued August 7, 2018.

Results of Evaluation

To determine the extent to which the Department's cloud-computing security controls prevent the loss of sensitive data hosted by CSPs, we selected a key Department cloud-based system for detailed testing. We found that the Department failed to implement and regularly test required controls to protect sensitive data contained in the system from unauthorized access.

We also reviewed cloud-computing security controls and found that the Department did not have a complete inventory of its cloud-based systems and did not ensure that bureaus purchased services using procurement contracts and from FedRAMP-approved CSPs. These deficiencies occurred because the Department:

1. Did not ensure the effectiveness of the cloud-based system's DLP controls.

2. Allowed employees to bypass the Department's Cloud Program Office when acquiring cloud-computing systems with purchase cards.

3. Did not impose penalties when CSPs failed to meet contractually required service levels.

We acknowledge that the Department has improved its acquisition and implementation of cloud-computing services since our prior evaluation in 2015. Nonetheless, weaknesses in the Department's cybersecurity program, including in cyber risk management, contractor oversight, and cloud procurement practices, put sensitive personally identifiable information (PII) at high risk of unauthorized access and potentially impeded the Department from fully realizing the benefits of moving its systems' data into a cloud. A PII breach of Department CSP-hosted data could cost the Department millions of dollars for credit-monitoring services and erode public trust.

Security Controls Did Not Prevent Loss of Sensitive PII

According to the Department, the cloud-based system we selected for testing contains sensitive PII for both Department and non-Department Federal employees. Sensitive PII could include, for example, names, social security numbers, biometric data records, credit card information, date and place of birth, or mother's maiden name. The system has been authorized to operate in a cloud for several years. Moreover, the Department has designated the system as a high-value asset.[20] High-value assets are systems that often contain sensitive data or support mission-critical operations. A breach of a high-value asset can be expected to have a serious adverse effect on Department operations and may result in the loss of sensitive data.

We selected the subject system for technical testing because of its designation as a high-value asset; it is imperative to ensure that this system is well-protected given the significant amount of

[20] According to the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency, a high-value asset is information or an information system that is so critical to an organization that the loss or corruption of this information or loss of access to the system would have serious impact to the organization's ability to perform its mission or conduct business. https://www.cisa.gov/sites/default/files/publications/CISAInsights-Cyber-SecureHighValueAssets_S508C.pdf.

sensitive data stored in this cloud system. According to the system security plan, the Department is responsible for the DLP solution, incident detection, and handling security controls. As a recognized best practice, an effective DLP capability captures and monitors network traffic in real time and performs content inspection such as rule-based analysis to identify sensitive PII. If sensitive data are detected, the DLP solution should block the traffic to prevent data loss (see Figure 1). The DLP solution should also generate alerts in real time to notify IT security analysts to determine whether the organization's computer network may have been breached or infected with malware.

Figure 1: How an Effective Data Loss Prevention (DLP) Solution Works

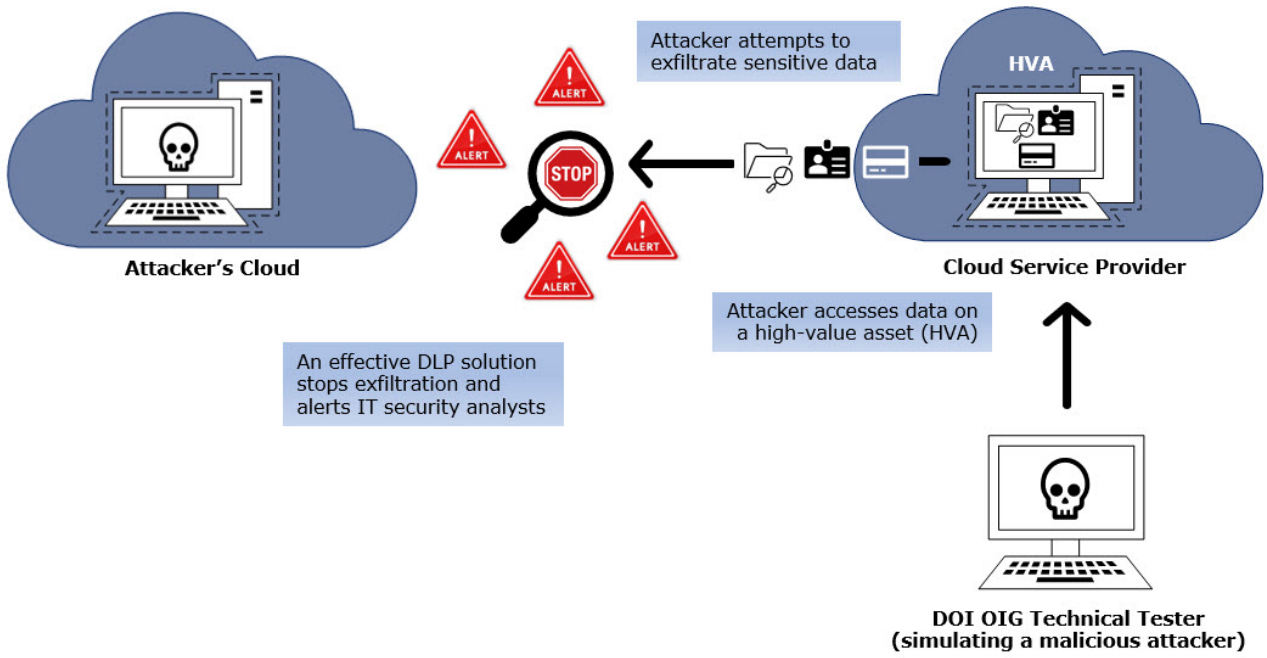

Figure 1 depicts how an effective DLP solution would prevent exfiltration of sensitive data. If a Department of the Interior (DOI) OIG Technical Tester, simulating a malicious attacker, accesses data on a high-value asset hosted by a cloud service provider and were to attempt to exfiltrate sensitive data, having an effective DLP solution in place would reduce the risk of successful exfiltration and alert IT security analysts of the attempt to exfiltrate.

Source: DOI OIG (alert icon by Omeris/stock.adobe.com and stop sign icon by martialred/stock.adobe.com; all other icons are by Microsoft).

As part of a weeklong data security test, we conducted technical testing of the DLP solution using fictitious PII. We used a publicly available web application to generate our fictitious sensitive PII.[21] The PII was created using appropriate rules necessary to create data that would appear valid to the Department's security tools.

[21] We obtained test data used as part of the exfiltration exercise from https://mockaroo.com/, which is widely used for generating test data.

We used well-known and widely documented techniques to exfiltrate data sets of 100, 1,000, or 10,000 records. We conducted our tests from a virtual machine running inside the subject system[22] and the account used to perform the tests did not have elevated or special privileges. Instead, to imitate a sophisticated threat actor, we used the virtual machine as-is and did not install any tools, software, or malware that would make it easier to exfiltrate data from the subject system.

We found that the Department's DLP solution did not prevent or detect our exfiltration tests (see Figure 2). We successfully exfiltrated more than a gigabyte of sensitive PII, containing more than 30 million fictitious sensitive PII records from the subject system.[23]

Figure 2: Technical Testing of Cloud Systems' Data Loss Prevention Controls

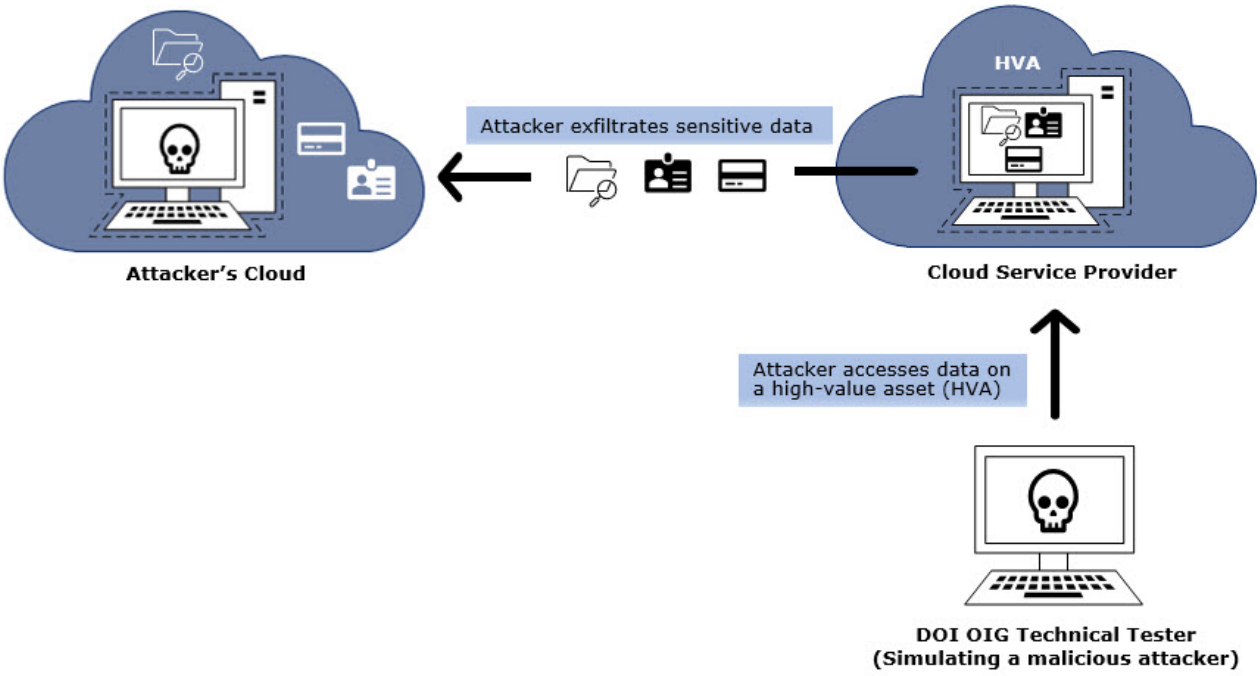

Figure 2 depicts how a DOI OIG Technical Tester, simulating a malicious attacker, accessed data on a high-value asset hosted by a cloud service provider. The attacker then exfiltrated sensitive PII from the cloud-hosted system and stored the data in the attacker's cloud. The exfiltration was possible because there was not an effective DLP solution in place.

Source: DOI OIG.

[22] A virtual machine is a digital version of a physical computer. Like a physical computer, a virtual machine can run programs and operating systems, store data, connect to networks, and perform other computing functions.

[23] The Department provided us with a copy of the subject system to ensure that our testing would not disrupt bureau operations. The system against which we performed tests contained the same data and had the same security controls as the production system.

The rules of engagement[24] allowed the Department to take action to deny the computer performing the tests to have continued access to the subject system, a step that would have immediately ended the test. As we performed the tests, we monitored the Department's security logs and incident tracking system in real time to see whether its DLP solution detected our exfiltration tests by either preventing the exfiltration or generating security alerts that would have triggered the Department's incident response process. However, our more than 100 exfiltration tests went undetected and were not blocked by the DLP solution; accordingly, our tests did not trigger the Department's security incident response process. We note that our final exfiltration test was specifically designed to trigger the Department's security incident response process; this test did not employ any of the previously stated tactics malicious actors use to avoid detection. The final test also went undetected, and we exfiltrated a gigabyte of fictitious PII.

Our tests succeeded because the Department failed to implement a DLP solution capable of detecting well-known and widely used techniques employed by malicious actors to steal sensitive data. Moreover, since the subject system has been hosted in a cloud, the Department has never conducted regular tests of the system's DLP controls, as required by NIST SP 800–53A, to ensure they were implemented correctly, operating as intended, and producing the desired outcome of protecting sensitive PII housed in the subject system from unauthorized access.[25] A PII breach of the subject system, which is a high-value asset, can be expected to have a serious or severe adverse effect on Department operations and could also cost the Department millions of dollars in credit-monitoring services, which are typically offered after such breaches.

While our testing identified the DLP concerns above, our tests also verified that a key security measure operated as intended. Specifically, internet-bound system traffic was routed through a trusted internet connection (TIC)[26] as a security measure to help prevent a malware-infected computer from receiving instructions from a command-and-control computer server[27] operated by a malicious actor. We simulated an infected host inside the subject system attempting to contact known malware command-and-control sites. Each of the dozens of attempts we made to connect to these malicious sites were blocked by either the TIC (i.e., the Cybersecurity and Infrastructure Security Agency) or by the Department.

[24] Rules of engagement define detailed guidelines and constraints regarding the execution of information security testing. The rules are established before the start of a security test and give the test team authority to conduct defined activities without the need for additional permissions. https://csrc.nist.gov/glossary/term/rules_of_engagement.

[25] NIST SP 800–53A, Revision 4, *Assessing Security and Privacy Controls for Federal Information Systems and Organizations*, December 2014.

[26] The TIC initiative was established to help redefine Federal cybersecurity by consolidating network connections and enhancing visibility and security measures throughout the Federal network.

[27] A command-and-control server is a computer controlled by an attacker, which is used to send commands to computers compromised by malware to, for example, receive stolen data from a target network.

Recommendations

We recommend that the Office of the Chief Information Officer:

1. Extend the capability of its data loss prevention solution to include rule-based analysis to detect and prevent the exfiltration of sensitive data from the subject system in accordance with industry best practices.

2. Regularly test the Department's data loss prevention capability to ensure that sensitive data in the subject system is protected against data exfiltration attempts.

3. Evaluate data communication protocols in use by the subject system that are vulnerable to exploitation and implement controls to mitigate identified vulnerabilities.

4. Ensure the implementation and annual testing of contractually required data loss prevention controls on all cloud systems containing sensitive data.

The Department Has Not Implemented Controls To Ensure Cloud-Computing Services Are Acquired According to Policy, Inventoried, and FedRAMP Approved

According to the Department's cloud procurement process, bureau or office staff seeking to procure cloud services must register a procurement request with the Department Cloud Program Office.[28] Once the Cloud Program Office registers this request, it is responsible for ensuring a FedRAMP-approved service is acquired and a technical readiness assessment is conducted. Finally, the cloud service must be procured using a cloud services contract that the cloud officer has approved and vetted.[29] If an approved cloud services contract does not satisfy mission needs, the Cloud Program Office may grant a waiver to allow the bureau or office to procure cloud services using micropurchase authority (i.e., Department purchase card). As part of the registration and approval process, the bureau or office is required to add the Department cloud service to the Department Cloud Program Office's inventory.

As part of our 2015 evaluation of the Department's cloud-computing practices, we found that all cloud services procured through the contracting process were from FedRAMP-approved

[28] OCIO Directive 2021–001, *Registration of Public Cloud Applications/Instances*, dated April 9, 2021, "requires bureaus and offices to register all the public cloud instances procured through third party vendors." Bureaus are directed to register their public cloud instances with the Department's "Cloud Inventory Database CIMS," which includes a field for providing the FedRAMP Package ID.

[29] The Cloud Services Request Process document dated March 29, 2022, outlines the OCIO process for requesting cloud services and the steps taken before approval is granted to either use an existing enterprise solution, acquire the cloud service through the FCHS acquisition process, or acquire the cloud service via a waiver.

providers and were included in the information system inventory.[30] We also found, however, that none of the 16 cloud services acquired using purchase cards were included in the Department's information system inventory, and none met Federal and Department IT security requirements.[31] As a result, we recommended that the Department migrate cloud services acquired through purchase cards to an approved cloud service contract and prohibit the future use of micropurchase authority when acquiring cloud services. The Department concurred with both recommendations and issued policy in 2015 prohibiting the use of micropurchase authority to acquire cloud-computing services. Accordingly, we closed this recommendation.

In 2021, however, the Department modified the policy to permit an exception allowing warranted contracting officers to use micropurchase authority to acquire cloud services. The policy specifically provides that warranted contracting officers using Department purchase cards are responsible for ensuring that approvals or waivers are obtained for these transactions, and a corresponding process was put into place. Accordingly, when the Department Cloud Program Office's process for requesting cloud services is followed, only a FedRAMP-approved cloud service can be authorized for acquisition, either via the FCHS acquisition process or via a waiver. The policy also requires the cloud services to be registered with the Cloud Program Office and preapproved by the Department CIO or the respective bureau or office Director of Information Resources, as appropriate.

We reviewed purchase card transactions from January 1, 2016, through April 27, 2022, and found 2,352 transactions, totaling $667,513, associated with established cloud-computing technology vendors. Of the 2,352 transactions, 2,118 were placed before the effective date of the waiver process; in these instances, bureaus easily bypassed controls to acquire cloud services using purchase cards. In particular, bureaus were able to acquire cloud services using Department purchase cards, which was prohibited under the previous charge card policy.

In addition, we judgmentally selected a sample of purchase card transactions spanning the past 3 years and found that 87 percent (7 of 8) transactions were not registered with the Department Cloud Program Office at the time of purchase. Registering with the Department Cloud Program Office helps ensure that any acquisitions for cloud services meet Federal and Department cloud security requirements. Because offices and bureaus did not follow the OCIO's process when originally acquiring the services, the purchases may not have been for FedRAMP-approved products. For example, one CSP that provided cloud services does not currently offer FedRAMP-approved services, and another CSP did not offer FedRAMP-approved services at the time of the purchase. While the remaining six CSPs offer specific FedRAMP-approved products,

[30] *The U.S. Department of the Interior's Adoption of Cloud Computing Technologies* (Report No. ISDN–EV–OCI–0002–2014), issued May 2015.

[31] OCIO Directive 2011–006, *Information System Boundary Assessment & Authorization Package Documentation and Inventory*, dated March 23, 2011, introduced Cyber Security Assessment and Management (CSAM) as the official information system inventory repository to be used by the Department of the Interior's bureaus and offices for system boundary assessment and authorization, tracking of weaknesses and corrective action plans, quarterly and annual FISMA performance metrics reporting, and annual IT Security Assessments. These requirements are separate from and address different issues than does the FedRAMP process. This directive was rescinded on April 25, 2023, because the Department of the Interior is replacing the CSAM system with a new Governance, Risk, and Compliance (GRC) information system to be known as Bison GRC. Once Bison GRC is fully implemented and capable of meeting its intended compliance requirements and access to the CSAM system is no longer required, the new system will become the Department's official information system security compliance solution and the CSAM system will be officially decommissioned.

we were unable to determine if offices and bureaus acquired products that were FedRAMP-approved because they did not follow the OCIO's process that would have allowed this assessment.

These deficiencies occurred because the OCIO failed to ensure that adequate controls were developed and implemented to prevent or promptly detect the purchase and use of cloud-computing services by Department employees using purchase cards. As noted previously, in response to Recommendation 6 from our 2015 evaluation, the Department policy was updated to prohibit the acquisition of cloud services on a charge card. We found that the 2021 policy update allowing the purchase of cloud services on charge cards if there is an approved waiver has in fact made it more difficult for the Department to determine whether cloud services have been purchased outside of the authorized process. In particular, under the previous policy prohibiting all cloud services from being purchased on purchase cards, any cloud service acquisition via a purchase card would be unauthorized. With the updated policy, cloud service purchases are allowed by purchase card in some situations, but there is no corresponding process that requires correlation of the purchase of cloud-computing services on a purchase card to an approved waiver; moreover, there is no process to identify which cloud service acquisitions on a purchase card were authorized with a waiver. In addition, an official from the Cloud Program Office stated that there is no mechanism available to prevent purchases from being approved at the time of sale even if a waiver has not been obtained. This issue becomes particularly complex because many purchases of this type may recur monthly or annually.

Further, the Department's controls failed to ensure that cloud services acquired with purchase cards were FedRAMP-compliant and properly added to the Department's information system inventory once purchased. This leads to a variety of potential problems. Information systems that are not included in the Department's inventory are not visible to the OCIO, which is responsible for ensuring the security of all information systems that Department employees and contractors use on behalf of the Government. Cloud-computing systems not included in the Department's inventory will not undergo the Department's information security accreditation and authorization process. Cloud-computing systems that are not included in the Department's inventory may also be omitted from required Federal annual reports, such as the Federal Information Security Modernization Act (FISMA) report and the report to the Federal CIO concerning cloud services that cannot meet FedRAMP security requirements.[32] Finally, cloud-computing systems that are not included on the Department's inventory with a valid operational status will not be included in the Office of Inspector General's yearly independent review of information security practices.[33] These reports identify deficiencies and promote accountability to ensure that the Department's systems are meeting Federal security requirements—a necessary step to safeguarding PII and other sensitive data.

[32] The 2011 OMB FedRAMP memo requires the agency to "provide to the Federal Chief Information Officer (CIO) annually on April 30, a certification in writing from the Executive department or agency CIO and Chief Financial Officer, a listing of all cloud services that an agency determines cannot meet the FedRAMP security authorization requirements with appropriate rationale and proposed resolutions."

[33] As part of the FISMA performance audit, a subset of Department information systems is selected from the Department's CSAM system for assessment of the effectiveness of the Department's information security program and practices and the implementation of the security controls. The CSAM system is the official repository of information systems and documentation for security authorization processes in the risk management framework.

Without accurate and complete inventories, the Department does not know the extent to which its data reside outside its system boundaries and are subject to the risks of cloud systems. These risks include isolation failure, interception of data in transit, and insecure or ineffective deletion of data. If exploited, these risks expose the Department's data to unauthorized parties and potentially compromise the objectives of Department programs. In addition, security controls for these seven cloud services were not required to be tested in a timely manner to ensure controls were implemented correctly, operating as intended, and producing the desired outcome of protecting the systems and their data.

Finally, when offices and bureaus do not follow the OCIO's process when purchasing cloud-based services, recommended best practices—such as clearly defined roles and responsibilities of the parties—Federal privacy, data production, and retention and destruction requirements might not be addressed. In addition, if Department offices and bureaus use a CSP's default service contract instead of an approved procurement contract, such as an FCHS contract, the CSP may be in a position to unilaterally modify contract terms without notifying the Department.[34] The terms and conditions of the CSP's default service contract rather than a service contract approved by the OCIO may put the Department data stored in the cloud at increased risk of compromise and increases the likelihood that public funds may be misspent.

Recommendations

We recommend that the Office of the Chief Information Officer:

5. Establish controls to identify, detect, and prevent unauthorized cloud services when they are acquired and used outside of the Office of the Chief Information Officer's process.

6. Issue formal guidance to all Department employees and contractors detailing the Office of the Chief Information Officer's approved processes, procedures, and requirements for acquiring authorized cloud-computing services.

7. Establish a process to regularly review purchase card transactions to identify and ensure that all cloud-computing systems used by Department employees and contractors on behalf of the Department are included in the Department's authoritative information system inventory.

8. Establish controls to ensure that only FedRAMP-approved cloud-computing services are authorized to access the Department's network and that non-FedRAMP-approved cloud-computing services in use are discontinued and blocked from access to Department network resources in accordance with the Department's acceptable use policy.

[34] In our previous evaluation, *The U.S. Department of the Interior's Adoption of Cloud Computing Technologies*, we noted that when a purchase card was used to acquire cloud services, the default service contract was accepted, 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.

Contracts With CSPs Included Many Recommended Best Practices But Can Be Improved

We selected a sample of eight contracts used to acquire cloud-computing services to determine whether they met OCIO requirements and best practices for acquiring cloud services as recommended by Federal CIOs and Chief Acquisition Officers (CAOs) and FedRAMP's security assessment framework.[35] The OCIO requires all cloud acquisitions to include these security requirements within the contract award.[36] Each system we selected had a Federal Information Processing Standards ratings of "Moderate," meaning the cloud system's loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on Department operations, assets, or individuals. Specifically, we evaluated whether the contracts contained language concerning 11 best practices for protecting Federal data:

- Defined roles and responsibilities of all parties;
- Guaranteed system availability levels;
- Reporting of service-level metrics;
- Penalties for not meeting service levels;
- E-discovery (requirements to locate, preserve, collect, process, and produce electronic data);
- Data retention and destruction policies;
- Data loss prevention;
- Data privacy requirements;
- Defined incident-handling practices;
- NIST encryption requirements; and
- Third-party certification of IT security programs.

We found that 7 of 8 contracts reviewed contained a majority of the 11 best practices for cloud-computing contracts recommended by Federal CIOs and CAOs and FedRAMP's security assessment framework. However, none of the contracts had clauses enforcing penalties when CSPs did not meet contractually required service-level metrics. Specifically, contracts for cloud services should clearly define how service levels are guaranteed (such as response time, resolution

[35] FedRAMP, "Creating Effective Cloud-Computing Contracts for the Federal Government: Best Practices for Acquiring IT as a Service," issued February 2012.

[36] Department memorandum, *Acquisition of Information Technology Cloud Services/Mandatory Use of Pre-Approved Cloud Hosting Services and Contracts*, issued August 7, 2018.

or mitigation time, and system availability) and require providers to monitor their service levels and provide timely reporting of failures to meet service levels. Moreover, contracts should include enforcement mechanisms that prescribe penalties when service levels are not met. We note that none of the contracts that we reviewed contained any enforcement mechanisms for failure to comply with contractual standards.

Further, many of the best practices discussed above are also incorporated directly or indirectly within OCIO requirements. For example, ACIOs are responsible for ensuring that the cloud procurements include requirements such as: (1) service-level metrics reporting; (2) penalties for not meeting service level metrics; (3) Controlled Unclassified Information (CUI) requirements as specified in 32 C.F.R part 2002; and (4) all other IT security and privacy requirements as specified in the existing FCHS contract.[37]

Because none of the contracts prescribed penalties for failure to meet agreed-upon service levels, the Department has no assurance that respective CSPs meet required service levels, which increases the risk of public funds being misspent by paying for a level of service that a CSP has not met.

In addition, two of the eight contracts we reviewed were missing multiple best practices. Specifically, the contract for the Legal Hold Pro system, which did not use an FCHS contract, was missing three recommended contract elements. Another contract that did not use an FCHS contract, the Recreation Business Management System contract, failed to include two recommended contract elements. Missing elements included penalties for not meeting service-level agreements and E-discovery requirements.

In our 2015 evaluation of the Department's cloud-computing practices, we performed a similar exercise and found that the four cloud-computing contracts we reviewed failed to contain many recommended best practices, along with OCIO requirements. We recommended that the Department:

1. Establish specifications to be incorporated in all contracts with CSPs to mitigate business and IT security risks inherent to cloud-computing environments.

2. Modify FCHS to incorporate Federal data retention and destruction policies, 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 CIO and CAO Councils.

4. Migrate all existing contracts for cloud services to FCHS or modify the contracts to incorporate best practices for procuring cloud services as recommended by the CAO and CIO Councils.

[37] Department memorandum, *Acquisition of Information Technology Cloud Services/Mandatory Use of Pre-Approved Cloud Hosting Services and Contracts*.

The Department concurred with and subsequently issued policy to implement the recommendations. We accordingly designated these recommendations as "closed." However, based on the results of our current review, we found that the corrective action taken to resolve our prior recommendations did not sufficiently address Recommendations 2 and 4. As described in our previous report, failure to ensure that all requirements are included in cloud-computing contracts increases business and security risks for Department data that are processed, transmitted, and stored in the cloud. Consequently, we are making two new recommendations to specifically address the deficiencies we identified.

Recommendations

We recommend that the Office of the Chief Information Officer:

9. Modify its Foundation Cloud Hosting Services contract to incorporate penalties for not meeting service-level agreements.

10. Ensure all existing non-Foundation Cloud Hosting Services contracts are migrated to an approved enterprisewide cloud-hosting procurement or modified to incorporate OCIO requirements and best practices for procuring cloud services, as recommended by the Chief Acquisition Officer and Chief Information Officer Councils and OCIO policy.

Conclusion and Recommendations

Conclusion

In the current cyber threat environment, Federal agencies must implement robust DLP capabilities to prevent sensitive data in the cloud from loss to data exfiltration campaigns. Without such measures, sensitive Federal data in the cloud will be at high risk of unauthorized access by sophisticated, well-resourced adversaries. For example, the reported July 2023 compromise of a major software company's cloud by what was described as a Chinese APT group was said to result in the loss of 60,000 emails of State Department employees.

The Department has improved its acquisition and implementation of cloud-computing services since our prior evaluation in 2015. As the Department expands its use of cloud services, actions such as strengthening its governance and risk management practices could help mitigate the chances that Department operations could be disrupted, data lost or compromised, or public funds misused. Moreover, improved coordination between the Department's CIO and its bureaus and offices could ensure that unauthorized and unsecured cloud-computing services are not implemented, and that cloud-computing contracts incorporate best practices, while meeting all FedRAMP requirements.

We make the following recommendations to the OCIO to mitigate business and IT security risks and strengthen IT governance practices pertaining to cloud computing.

Recommendations Summary

We provided a draft of this report to the OCIO for review. The OCIO concurred with Recommendations 1 through 7 and Recommendations 9 and 10. It partially concurred with Recommendation 8. We consider Recommendations 1 through 7 and Recommendations 9 and 10 resolved. We consider Recommendation 8 unresolved. We independently modified our draft report and certain recommendations to omit potentially sensitive information and also redacted information from the OCIO's response for the same reason. Below we summarize the OCIO's response to our recommendations and our comments on its response. See Appendix 3 for the full text of the OCIO's response; Appendix 4 lists the status of each recommendation.

We recommend that the Office of Chief Information Officer:

1. Extend the capability of its data loss prevention solution to include rule-based analysis to detect and prevent the exfiltration of sensitive data from the subject system in accordance with industry best practices.

   OCIO's Response: The OCIO concurred with the recommendation and stated that it will implement "more robust rules and hybrid controls" for DLP. The OCIO provided a target implementation date of December 15, 2024.

OIG Comment: Based on the OCIO's response, we consider Recommendation 1 resolved. The recommendation will be considered implemented when we receive positive results from OIG retesting of the DLP controls.

2. Regularly test the Department's data loss prevention capability to ensure that sensitive data in the subject system is protected against data exfiltration attempts.

   OCIO's Response: The OCIO concurred with the recommendation and stated that it will implement a "robust DLP Test Plan that will also establish regular testing cycles and reporting." The OCIO provided a target implementation date of March 31, 2024.

   OIG Comment: Based on the OCIO's response, we consider Recommendation 2 resolved. The recommendation will be considered implemented when we receive evidence of successful regular testing of DLP controls and remediation of any areas of improvement identified during these tests.

3. Evaluate data communication protocols in use by the subject system that are vulnerable to exploitation and implement controls to mitigate identified vulnerabilities.

   OCIO's Response: The OCIO concurred with the recommendation and stated that it will implement controls to mitigate identified data communication protocol vulnerabilities. The OCIO provided a target implementation date of June 30, 2024.

   OIG Comment: Based on the OCIO's response, we consider Recommendation 3 resolved. The recommendation will be considered implemented after we review the OCIO's mitigations and retest the DLP controls with positive results.

4. Ensure the implementation and annual testing of contractually required data loss prevention controls on all cloud systems containing sensitive data.

   OCIO's Response: The OCIO concurred with the recommendation and stated that it will review DLP-related controls testing for FedRAMP cloud systems containing sensitive data at least annually and report any deficiencies to contracting officers for inclusion in the Contractor Performance Assessment Reporting System. The OCIO provided a target implementation date of June 30, 2024.

   OIG Comment: Based on the OCIO's response, we consider Recommendation 4 resolved. The recommendation will be considered implemented when the OCIO provides supporting documentation that demonstrates that it has established a process to ensure annual testing and that it has conducted appropriate reviews of DLP controls.

5. Establish controls to identify, detect, and prevent unauthorized cloud services when they are acquired and used outside of the Office of the Chief Information Officer's process.

   OCIO's Response: The OCIO concurred with the recommendation and stated that, along with the steps that it will take to implement Recommendation 7, it will evaluate (a) technical controls to detect new cloud networks and (b) Federal IT Acquisition Reform Act policy to prevent unapproved cloud purchase card transactions. The OCIO's target implementation date is December 15, 2024.

   OIG Comment: Based on the OCIO's response, we consider Recommendation 5 resolved. The recommendation will be considered implemented when we receive evidence that the OCIO has implemented controls that identify, detect, and prevent unauthorized cloud services.

6. Issue formal guidance to all Department employees and contractors detailing the Office of the Chief Information Officer's approved processes, procedures, and requirements for acquiring authorized cloud-computing services.

   OCIO's Response: The OCIO concurred with the recommendation. It stated that the OCIO and the Office of Acquisition and Property Management will "jointly review governance roles and responsibilities for cloud acquisition services and will reissue formal guidance to all Department employees and contractors detailing the approved processes, procedures, and requirements." The OCIO's target implementation date is October 31, 2024.

   OIG Comment: Based on the OCIO's response, we consider Recommendation 6 resolved. To date, the OCIO has not provided the OIG with evidence that it has issued or reissued any formal guidance that would meet the requirements of this recommendation. The recommendation will be considered implemented when we received such guidance and confirm that it includes appropriate and clearly defined processes, procedures, and requirements for acquiring cloud-computing services.

7. Establish a process to regularly review purchase card transactions to identify and ensure that all cloud-computing systems used by Department employees and contractors on behalf of the Department are included in the Department's authoritative information system inventory.

   OCIO's Response: The OCIO concurred with the recommendation and stated that it has implemented a monthly review of purchase charge transactions to identify cloud services as of July 2023. It summarized this approach in its response. Further, the OCIO stated that it "will ensure the new policy will request qualified cloud services be included in the Department's authoritative information system inventory." The OCIO provided a target implementation date of June 30, 2024.

OIG Comment: Based on the OCIO's response, we consider Recommendation 7 resolved. The recommendation will be considered implemented when the OCIO provides evidence that is has established and implemented a process for review of the purchase card transactions on a monthly basis and made any updates to the information system inventory for cloud services as defined by NIST.

8. Establish controls to ensure that only FedRAMP-approved cloud-computing services are authorized to access the Department's network and that non-FedRAMP-approved cloud-computing services in use are discontinued and blocked from access to Department network resources in accordance with the Department's acceptable use policy.

   OCIO's Response: The OCIO partially concurred with the recommendation and stated that the Department generally complies with FedRAMP-approved cloud-computing services. It stated, however, that there are "permissible exceptions" under the FedRAMP Authorization Act for cloud services that an agency determines cannot meet the FedRAMP security authorization requirements. The OCIO stated that it considers this recommendation to have been implemented as of April 30, 2023.

   OIG Comment: Based on the OCIO's response, we consider Recommendation 8 unresolved. The OCIO's response did not address its plan to establish controls and discontinue or block unauthorized services. The recommendation will be considered implemented when the OCIO demonstrates that it has implemented controls to ensure that only FedRAMP-approved cloud-computing services are allowed to access the Department's network and that non-FedRAMP-approved cloud-computing services have been discontinued and blocked from accessing the Department's network. If the OCIO determines that there are permissible exemptions, it should provide documentation that all of these exemptions are allowable and reported in accordance with FedRAMP.

9. Modify its Foundation Cloud Hosting Services contract to incorporate penalties for not meeting service-level agreements.

   OCIO's Response: The OCIO concurred with the recommendation and stated that it intends to award a new Foundational Cloud Services Contract that incorporates penalty clauses into the service-level agreement. The OCIO provided a target implementation date of December 15, 2024.

   OIG Comment: Based on the OCIO's response, we consider Recommendation 9 resolved. The recommendation will be considered implemented when penalties for failing to meet services levels are included the Foundation Cloud Hosting Services contract.

10. Ensure all existing non-Foundation Cloud Hosting Services contracts are migrated to an approved enterprisewide cloud-hosting procurement or modified to incorporate OCIO requirements and best practices for procuring cloud services, as recommended by the Chief Acquisition Officer and Chief Information Officer Councils and OCIO policy.

    OCIO's Response: The OCIO concurred with the recommendation and stated that it will migrate current task orders as they expire to approved contracts. The OCIO provided a target implementation date of December 15, 2025.

    OIG Comment: Based on the OCIO's response, we consider Recommendation 10 resolved. The recommendation will be considered implemented when the OCIO provides support demonstrating that all task orders are moved to approved enterprisewide contracts or modified to incorporate OCIO requirements and best practices for procuring cloud services.

Appendix 1: Scope and Methodology

Scope

We evaluated the Department's cloud-computing security controls from March 2022 to June 2023 to determine whether they were adequate to prevent unauthorized access, modification, or destruction of data as required by Federal policies and industry best practices.

Methodology

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

To accomplish our evaluation objectives, we performed the following:

- Interviewed Department, bureau, and office personnel and cloud system owners.

- Reviewed the Federal Cloud Computing Strategy, Office of Management and Budget guidance, National Institute of Standards and Technology criteria, Best Practices of the Chief Acquisition Officers (CAO) and Chief Information Officers (CIO) Councils, and Federal Risk and Authorization Management Program (FedRAMP) requirements.

- Evaluated Department policies and procedures related to Department purchase cards, acquisition of cloud-computing technology, and cloud-computing security.

- Examined system security plans and the inventory of cloud-based resources to perform contract analysis and technical testing based on system criticality; type of cloud service—Infrastructure as a Service (IaaS), Platform as a Service (PaaS), or Software as a Service (SaaS); application usage; and sensitivity of hosted data.

- Performed technical testing of data loss prevention controls for the subject system by emulating a malicious actor using well-known techniques to exfiltrate fictitious sensitive personally identifiable information from the production environment.

- Judgmentally selected a sample of eight contracts, prioritizing the type of cloud service (IaaS, PaaS, or SaaS) and sensitivity of hosted data, and determined whether the sample of contracts with the Department's cloud service providers incorporated best practices recommended by the CAO and CIO Councils for mitigating risks associated with cloud-computing environments.

- Determined what mechanisms are in place at the Department Cloud Program Office to identify all providers and brokers of cloud services with deployments across the Department.

- Analyzed purchase card transaction data to determine whether cloud services were purchased using purchase cards in accordance with Department policies and included in the information system inventory. We judgmentally selected a sample of eight transactions for further testing via a questionnaire and purchase documentation review to determine whether the Office of the Chief Information Officer process for acquiring cloud-computing technology was followed.

- Conducted data analysis of purchase card transaction data to create a consolidating listing of total purchase card spending with established cloud vendors. We visited the online FedRAMP marketplace to determine which of the established cloud vendors identified have FedRAMP-certified products currently available.

Appendix 2: Status of Recommendations From 2015 Evaluation

Recommendation	Date Closure Requested	Status	Actions Taken
1. We recommend that the Department 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.	09/2016	Implemented	The Office of the Chief Information Officer (OCIO) worked with the Office of Acquisition and Property Management (PAM) to update the previously issued Mandatory Use policy. The updated guidance specifically states that any contract vehicle utilized to acquire cloud computing services incorporates best practices for procuring cloud services. A process for requesting a waiver to the policy has been implemented and waivers must be approved by both the Chief Information Officer and the PAM Director. In addition, the OCIO maintains a robust website for cloud-related information. The website includes a Reading Room which contains specifications and relevant attachments for Federal Cloud Hosting Services (FCHS) contracts.

Recommendation	Date Closure Requested	Status	Actions Taken
2. We recommend that the Department modify FCHS to incorporate Federal data retention and destruction [policies], including mechanism(s) to measure, report, and enforce contractor performance metrics.	07/2015	Implemented*	OCIO developed a Statement of Work template that is utilized by the Cloud Hosting Program Management Office. The template is used to develop requirements for each task issued against the FCHS contract. The template was altered to incorporate Federal data retention and destruction policies and include mechanisms to measure, report, and enforce contractor performance metrics. Supporting documentation includes numerous modifications to existing FCHS contacts which incorporate the required metrics.
3. We recommend that the Department 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.	09/2016	Implemented	The OCIO worked with PAM to update the previously issued Mandatory Use policy. The updated guidance specifically states that any contract vehicle utilized to acquire cloud computing services incorporates best practices for procuring cloud services. A process for requesting a waiver to the policy has been implemented and waivers must be approved by both the Chief Information Officer and the PAM Director. In addition, OCIO maintains a robust website for cloud-related information. The website includes a Reading Room which contains specifications and relevant attachments for FCHS contracts.

Recommendation	Date Closure Requested	Status	Actions Taken
4. We recommend that the Department 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.	06/2019	Implemented*	OCIO worked with the bureaus to either migrate contracts to the FCHS or update their existing contracts with best practices language; established a governance committee to oversee exception waivers; established a website for the cloud program; and provided annual training to the acquisition community.
5. We recommend that the Department 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.	03/2018	Implemented	OCIO worked with PAM to ensure that all cloud services that were acquired through the Government charge card were either terminated or migrated to a different procurement vehicle. In addition, the U.S. Geological Survey took corrective actions to mitigate their related findings noted in the Office of Inspector General report.
6. We recommend that the Department prohibit use of Government micropurchase authority (e.g., Government integrated charge cards) to acquire Cloud-computing services.	01/2016	Implemented	OCIO worked with PAM to ensure the prohibition of micropurchase authority to acquire cloud-computing services was included in the charge card policy. The revised policy, although not specifically updated due to this matter, includes this prohibition.

* As described previously in this report, we found that the Department's policies and practices have changed since implementation of the corrective actions and corrective actions did not fully address all of the recommendations, therefore we made two new recommendations to specifically address the ongoing deficiencies we identified.

Appendix 3: Response

The Office of the Chief Information Officer's response to our draft report follows on page 32.

United States Department of the Interior

OFFICE OF THE SECRETARY
Washington, DC 20240
11/6/23

Memorandum

To: Mark Lee Greenblatt
Inspector General

Through: Darren B. Ash
Chief Information Officer
Office of the Chief Information Officer

DARREN ASH Digitally signed by DARREN ASH Date: 2023.11.03 15:06:55 -04'00'

From: Stanley F. Lowe
Chief Information Security Officer
Office of the Chief Information Officer

STANLEY LOWE Digitally signed by STANLEY LOWE Date: 2023.11.06 13:09:07 -05'00'

Subject: Response to Draft Evaluation Report - *Cloud Security Weaknesses at the U.S. Department of the Interior Could Result in Loss of Government Data (2022-ITA-025)*

Thank you for providing the Department of the Interior (Department, DOI) the draft Office of Inspector General (OIG) Report, *Cloud Security Weaknesses at the U.S. Department of the Interior Could Result in Loss of Government Data (2022–ITA–025)*. This memorandum including attachment(s) responds to the draft report and will be emailed to aie_reports@doioig.gov as requested.

If you have questions, please contact Stanley Lowe, Chief Information Security Officer, at [redacted]@ios.doi.gov and OCIO_Audit_Management@ios.doi.gov.

Attachment 1: Recommendations and Responses

cc: Deputy Chief Information Officers, Office of the Chief Information Officers (OCIO)
Naznin Rahman, Chief, Audit Management Division, Office of Financial Management
Bureau and Office Associate Chief Information Officers
Bureau and Office Associate Chief Information Security Officers
Bureau and Office Associate Chief Data Officers
Bureau and Office Associate Privacy Officers
Douglas Scoville, Chief, Governance Branch, OCIO
Richard Westmark, Chief, Compliance Management Section, OCIO

Recommendations and Management Responses to *Cloud Security Weaknesses at the U.S. Department of the Interior Could Result in Loss of Government Data (2022–ITA–025)*

Recommendation 1: Extend the capability of its data loss prevention solution to include rule-based analysis to detect and prevent the exfiltration of sensitive data from the [redacted] in accordance with industry best practices.

Response: Concur. The Department of the Interior (DOI, Department), Office of the Chief Information Officer (OCIO) will implement more robust rules and hybrid controls for data loss prevention (DLP).

Responsible Official: Chief Information Security Officer

Target Date: December 15, 2024

Correction: The Office of Inspector General (OIG) report states on page 10 that "[redacted] has been authorized to operate in a public cloud since [redacted]." - Actually, it is a government community cloud environment.

Recommendation 2: Regularly test the Department's data loss prevention capability to ensure that sensitive data in the [redacted] is protected against data exfiltration attempts.

Response: Concur. The DOI will develop and implement a robust DLP Test Plan that will also establish regular testing cycles and reporting in which [redacted] will participate.

Responsible Official: Chief Information Security Officer

Target Date: March 31, 2024

Recommendation 3: Evaluate data communication protocols in use by the [redacted] and implement controls to mitigate identified vulnerabilities.

Response: Concur. The DOI will identify data communication protocols in use by [redacted], and implement mitigations [redacted]

Responsible Official: Chief Information Security Officer

Target Date: June 30, 2024

Recommendation 4: Ensure the implementation and annual testing of contractually required data loss prevention controls on all public cloud systems containing sensitive data.

Response: Concur. The DOI will at least annually review DLP related controls testing for FedRAMP cloud systems containing sensitive data in use and report deficiencies to contracting officer(s) for Contract Performance Assessment Reporting System (CPARS) inclusion.

Responsible Official: Deputy Chief Information Officer for Program Management

Target Date: June 30, 2024

Recommendation 5: Establish controls to identify, detect, and prevent unauthorized cloud services when they are acquired and used outside of the Office of the Chief Information Officer's process.

Response: Concur. In addition to implementing recommendation 7, which reviews purchase card transactions, th e DOI will evaluate (a) technical controls to detect new cloud networks, and (b) FITARA policy to prevent unapproved cloud purchase c ard transactions.

Responsible Official: (a) Chief Information Security Officer

Responsible Official: (b) Deputy Chief Information Officer for Program Management

Target Date: December 15, 2024.

Recommendation 6: Issue formal guidance to all Department employees and contractors detailing the Office of the Chief Information Officer's approved processes, procedures, and requirements for acquiring authorized cloud-computing services.

Response: Concur. The Office of Acquisition and Property Management (PAM) office and OCIO will jointly review governance roles and responsibilities for cloud acquisition services and will reissue formal guidance to all Department employees and contractors detailing the approved processes, procedures, and requirements once the new process is approved by the DOI Information Management and Technology Leadership Team (IMTLT).

Responsible Official: Deputy Chief Information Officer for Program Management and Director, Office of Acquisition and Property Management (PAM)

Target Date: October 31, 2024

Recommendation 7: Establish a process to regularly review purchase card transactions to identify and ensure that all cloud-computing systems used by Department employees and contractors on behalf of the Department are included in the Department's authoritative information system inventory.

Response: Concur. The DOI will continue its monthly review of purchase card transactions, started in July 2023. As part of the process, PAM runs a custom rule in a charge card data and analytics tool that identifies transactions from a list of cloud companies that the OCIO maintains. PAM sends the identified transactions to the OCIO for review. Then OCIO compiles the raw transaction list and shares with bureau and offices who in turn verify the cloud services that are required to be maintained in the Department's authoritative information system inventory, Xacta.

Additionally, DOI will ensure the new policy will request qualified cloud services be included in the Department's authoritative information system inventory.

For clarification, FISMA (and DOI) do not require all Internet based applications (*web-tools*) to achieve an Authority to Operate nor be included in the authoritative source, Xacta. These *web-tools* are categorized outside National Institute of Standards and Technology (NIST) Special

Publications (SP) 800-145 and 500-322 definition of "cloud services". Cloud definitions that do not apply, for example, are non-data hosting web-tools, websites, social media, publications, and applications listed under Digtal.gov/Tool and Services.

Responsible Official: Deputy Chief Information Officer for Program Management and Director, Office of Acquisition and Property Management (PAM)

Target Date: June 30, 2024

Recommendation 8: Establish controls to ensure that only FedRAMP-approved cloud-computing services are authorized to access the Department's network and that non-FedRAMP-approved cloud-computing services in use are discontinued and blocked from access to Department network resources in accordance with the Department's acceptable use policy.

Response: Concur. Generally, the Department complies with the FedRAMP-approved cloud-computing services.

Non-Concur: To allow for permissible exceptions, Office of Management and Budget (OMB) provides for a few instances under the FedRAMP Authorization Act and identified in the OMB Memorandum (FEDRAMP memorandum) *Security Authorization of Information Systems in Cloud Computing Environments*.

- under Section 4d. Each Executive or agency shall by April 30th each year: *Provide to the Federal Chief Information Officer (CIO) annually on April 30, a certification in writing from the Executive department or agency CIO and Chief Financial Officer, a listing of all cloud services that an agency determines cannot meet the FedRAMP security authorization requirements with appropriate rationale and proposed resolutions.*

Additionally, FedRAMP authorization is only required for full XaaS cloud services described under the NIST SP-800-145 Definition of Cloud Computing guidance. See clarification under recommendation 7.

Responsible Official: Deputy Chief Information Officer for Program Management

Target Date: Implemented April 30, 2023

Recommendation 9: Modify its Foundation Cloud Hosting Services contract to incorporate penalties for not meeting service-level agreements.

Response: Concur. The DOI intends to award a new Foundational Cloud Services Contract II (FCSC2) as an IDIQ that incorporates penalty clauses into the service level agreement (SLA).

Responsible Official: Deputy Chief Information Officer for Program Management

Target Date: December 15, 2024

Recommendation 10: Ensure all existing non-Foundation Cloud Hosting Services contracts are migrated to an approved enterprise-wide cloud-hosting procurement or modified to incorporate OCIO requirements and best practices for procuring cloud services, as recommended by the

Chief Acquisition Officer and Chief Information Officer Councils and OCIO policy.

Response: Concur. The DOI will migrate current task orders as they expire to approved contracts which will substantially occur during Fiscal Years 2024 and 2025.

Responsible Official: Deputy Chief Information Officer for Program Management

Target Date: December 15, 2025.

Appendix 4: Status of Recommendations

Recommendation	Status	Action Required
2022-ITA-025-01 We recommend that the Office of the Chief Information Officer (OCIO) extend the capability of its data loss prevention solution to include rule-based analysis to detect and prevent the exfiltration of sensitive data from the subject system in accordance with industry best practices.	**Resolved**	We will track implementation.
2022-ITA-025-02 We recommend that the OCIO regularly test the Department's data loss prevention capability to ensure that sensitive data in the subject system is protected against data exfiltration attempts.	**Resolved**	We will track implementation.
2022-ITA-025-03 We recommend that the OCIO evaluate data communication protocols in use by the subject system that are vulnerable to exploitation and implement controls to mitigate identified vulnerabilities.	**Resolved**	We will track implementation.
2022-ITA-025-04 We recommend that the OCIO ensure the implementation and annual testing of contractually required data loss prevention controls on all cloud systems containing sensitive data.	**Resolved**	We will track implementation.

Recommendation	Status	Action Required
2022-ITA-025-05 We recommend that the OCIO establish controls to identify, detect, and prevent unauthorized cloud services when they are acquired and used outside of the OCIO's process.	**Resolved**	We will track implementation.
2022-ITA-025-06 We recommend that the OCIO issue formal guidance to all Department employees and contractors detailing the OCIO's approved processes, procedures, and requirements for acquiring authorized cloud-computing services.	**Resolved**	We will track implementation.
2022-ITA-025-07 We recommend that the OCIO establish a process to regularly review purchase card transactions to identify and ensure that all cloud-computing systems used by Department employees and contractors on behalf of the Department are included in the Department's authoritative information system inventory.	**Resolved**	We will track implementation.
2022-ITA-025-08 We recommend that the OCIO establish controls to ensure that only FedRAMP-approved cloud-computing services are authorized to access the Department's network and that non-FedRAMP-approved cloud-computing services in use are discontinued and blocked from access to Department network resources in accordance with the Department's acceptable use policy.	**Unresolved**	We will meet with the OCIO to further discuss resolution of this recommendation.

Recommendation	Status	Action Required
2022-ITA-025-09 We recommend that the OCIO modify its Foundation Cloud Hosting Services (FCHS) contract to incorporate penalties for not meeting service-level agreements.	**Resolved**	We will track implementation.
2022-ITA-025-10 We recommend that the OCIO ensure all existing non-FCHS contracts are migrated to an approved enterprisewide cloud-hosting procurement or modified to incorporate OCIO requirements and best practices for procuring cloud services, as recommended by the Chief Acquisition Officer and Chief Information Officer Councils and OCIO policy.	**Resolved**	We will track implementation.

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.

Who Is Protected?

Anyone 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.