Best Practices for Federal Agencies to Strengthen Cloud Security

March 2026

PREFACE

The best practices identified within this report are intended to aid Federal agencies with implementing cloud security in an effective manner.

Table of Contents

COUNCIL OF THE INSPECTORS GENERAL ON INTEGRITY AND EFFICIENCY

COUNCIL OF THE INSPECTORS GENERAL ON INTEGRITY AND EFFICIENCY

COUNCIL OF THE INSPECTORS GENERAL ON INTEGRITY AND EFFICIENCY

Executive Summary

Best Practices for Federal Agencies to Strengthen Cloud Security

What We Found

We identified six common best practice themes with 19 best practices for cloud security. The six common best practices are:

1. Agencies Should Provide Oversight of Cloud Service Providers
2. Agencies Must Protect and Monitor Their Data
3. Agencies Should Implement Effective Identity and Access Management Practices
4. Agencies Should Implement Effective Configuration Management Practices
5. Agencies Should Implement Effective Continuous Monitoring Controls
6. Agencies Should Implement Effective Assessment and Authorization Practices

Federal agencies can learn from the challenges and related recommendations identified by Offices of Inspectors General (OIGs) and the Government Accountability Office (GAO) to help secure their cloud-based systems.

What We Reviewed and Why

We conducted this review on behalf of the Federal Audit Executive Council's Cross-Cutting Issues Subcommittee which was established to support the Council of the Inspectors General on Integrity and Efficiency (CIGIE) Audit Committee by coordinating government-wide activities that promote economy and efficiency in Federal programs and operations and address areas of weakness and vulnerability regarding fraud, waste, abuse and mismanagement. The Subcommittee also supports CIGIE by assisting in its statutory responsibility to address integrity, economy and effectiveness issues that transcend individual Government agencies. In October 2023, the Subcommittee formed a working group consisting of representatives from six OIGs to begin a collaboration effort to inform Federal agencies of best practices and aid Federal agencies with implementing cloud security in an effective manner based on findings, recommendations and conclusions identified in Federal oversight reports.

We identified best practices that agencies can adopt to strengthen their cloud security posture based on findings identified in 35 reports issued by 19 OIGs and the GAO between 2014 and 2024. At the time of report issuance, the OIGs and GAO recommended corrective actions for the reported findings, and individual agencies may have already implemented the respective recommendations. Eight individuals from six participating OIGs including EPA, EXIM, DOI, USPS, NGA and FDIC conducted this review. The objective of our review was to identify best practices and lessons learned from past and current Federal oversight work performed related to cloud security to help guide Federal agencies to strengthen their overall security posture.

What We Recommend

The working group identified six common best practices with 19 individual best practice elements for implementing effective cloud security based on 35 OIG reports related to cloud security with common findings and related best practices, issued between 2014 and 2024. Agencies should learn from the results of these reports and incorporate the best practices identified by the working group.

Background and Objective

The National Institute for Standards and Technology (NIST) defines cloud computing as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. The term "cloud" applies to solutions that exhibit five essential characteristics of cloud computing, as defined by NIST: on-demand service, broad network access, resource pooling, rapid elasticity and measured service.[1]

The cloud is a vast online storage space where people and businesses store their files and applications, accessible from anywhere with an internet connection. The cloud also offers services, such as computing power, databases, networking, and software applications. The main purpose of the cloud is to provide on-demand access to computing resources and services over the internet. This includes a wide range of services such as servers, storage, databases, networking, software, analytics, and intelligence. The cloud empowers people and organizations to use these resources without having to manage physical servers or run software applications on their own computers.

Federal agencies today are faced with the need to accelerate their adoption of cloud services while ensuring the systems that support their missions are safe and secure while operating in the cloud. Agencies must also effectively implement cloud security and ensure that agency data maintained in the cloud is secure. Agencies are contending with modernizing legacy information systems that have increased maintenance costs, lack of available support and a decreased capacity to support mission objectives and goals by transitioning legacy systems to the cloud.

Cloud computing offers many benefits including the ability to buy services more quickly, drive cost savings, improve security and deliver mission-serving solutions faster. It also enables organizations to do more with less by eliminating their on-premises infrastructure with the reduction of services and staff to support that infrastructure. According to NIST, while cloud computing offers many benefits it also introduces additional areas of concern, including system complexity, shared-multi-tenancy environments, internet facing services and losing control over resources in a cloud service provider environment.[2] In addition, different security risks and vulnerabilities are introduced when migrating systems to the cloud. Control over cloud systems and applications will vary by cloud provider and delivery service type. While cloud computing offers many advantages, effective governance over cloud security practices must be in place to manage security risks appropriately.

In October 2023, the Federal Audit Executive Council's (FAEC) Cross-Cutting Issues Subcommittee formed a working group consisting of representatives from six participating OIGs to identify best practices for Federal agencies to strengthen their security posture for Cloud Security based on findings, recommendations and conclusions identified in Federal oversight reports. The objective of our review was to identify best practices and lessons learned from past and current Federal oversight work performed related to cloud security to help guide Federal agencies to strengthen their overall security posture. After a detailed review of related Office of Inspector General (OIG) and Government Accountability Office (GAO) reports issued between 2014 and 2024, the team identified six common best practices within the 35 Federal oversight reports reviewed. When these reports were originally

[1] NIST Special Publication (SP) 800-145, *The NIST Definition of Cloud Computing* (September 2011)
[2] NIST SP 800-144, *Guidelines on Security and Privacy in Public Cloud Computing* (December 2011)

published, the OIGs and GAO made recommendations to improve cloud security related findings. Individual agencies may have already implemented the respective recommendations. The team did not assess whether reported conditions remain, but highlighted the common findings to help all agencies improve or reinforce cloud security.

Summary of Cloud Security Best Practice Themes in the 35 OIG and GAO Reports Reviewed

The graphic below shows the best practice themes identified, and the number of related reports identified for each theme:

*Some reports included findings related to more than one best practice theme.

Cloud Security Best Practice Themes and Recommendations

The graphic below shows all cloud security best practices, and their related themes identified during our review:

Theme 1: Agencies Should Provide Oversight of Cloud Service Providers (CSP)	•1.1 Establish and Maintain an Inventory of Cloud Service Contracts •1.2 Include Relevant Cloud Security Clauses in CSP Contracts •1.3 Monitor CSP Performance and Include Enforcement Mechanisms in CSP contracts
Theme 2: Agencies Must Protect and Monitor Their Data	•2.1 Establish and Maintain an Accurate Data Inventory •2.2 Use Approved Cloud Services to Store and Share Data •2.3 Protect Personally Identifiable Information (PII) and Controlled Unclassified Information (CUI) Data from Unauthorized Disclosure
Theme 3: Agencies Should Implement Effective Identity and Access Management Practices	•3.1 Use a Centralized Identity and Access Management System •3.2 Enforce Multi-factor Authentication •3.3 Periodically Audit User Access Privileges •3.4 Disable User Access in a Timely Manner •3.5 Separate Production and Non-production Cloud Environments
Theme 4: Agencies Should Implement Effective Configuration Management Practices	•4.1 Establish and Maintain Baseline Configurations •4.2 Establish and Maintain a Complete and Accurate Asset Inventory
Theme 5: Agencies Should Implement Effective Continuous Monitoring Controls	•5.1 Prioritize Continuous Monitoring and Establish and Implement a Continuous Monitoring Process •5.2 Ensure All Security Artifacts are Maintained and Use All Available Information to Perform Continuous Monitoring •5.3 Take Appropriate Actions in Response to Continuous Monitoring Findings
Theme 6: Agencies Should Implement Effective Assessment and Authorization Practices	•6.1 Perform Security Accreditations and Authorizations •6.2 Develop and Update the Business Impact Assessment and System Security Plan •6.3 Fully Implement Security Controls, Perform Regular Assessments, and Remediate Flaws

Cloud Security Best Practices

Theme 1: Agencies Should Provide Oversight of Cloud Service Providers

The Federal government is one of the largest buyers of cloud technology, and cloud service providers (CSP)[3] offer agencies innovative products that help them save time and resources while meeting their critical mission needs. Government agencies generally procure cloud services through contracts with CSPs. Agencies may also use service level agreements, which are agreements under the umbrella of the overall contract, to communicate requirements to their selected CSPs.

In February 2012, the Federal Chief Information Officers (CIO) Council and Chief Acquisition Officers Council, in coordination with the Federal Cloud Compliance Committee, published a best practice guide for acquiring cloud services.[4] The guide brings together collective expert inputs that highlight unique contracting requirements related to cloud computing contracts to guide Federal agencies in effectively and safely procuring cloud services for agency consumption.

While agencies are ultimately responsible for securing and protecting their information and services in the cloud, the CSP and the agency share responsibility for implementing required security controls. Therefore, it is imperative that agencies effectively procure and manage cloud computing services through contracts with CSPs that sufficiently address business and security risks that include relevant security clauses and properly define and provide a mechanism to monitor and enforce CSP performance. In addition, it is also imperative that agencies establish and maintain an inventory of cloud service contracts to ensure that security risks related to operating in cloud environments are managed appropriately.

Of the 35 reports that the working group analyzed, 12 had findings related to cloud contract management and agency oversight of CSPs.

Recommended Best Practices:

1. We recommend that Federal agencies implement the following best practices for more effective oversight of CSPs:
   1.1 Establish and maintain an inventory of cloud service contracts.
   1.2 Include relevant cloud security clauses in CSP contracts.
   1.3 Monitor CSP performance and include enforcement mechanisms in CSP contracts.

1.1 Establish and Maintain an Inventory of Cloud Service Contracts

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.[5] Without a clear inventory of cloud

[3] CSPs are entities that may develop infrastructure, platform and software application services that can be shared by multiple customers. Each customer can buy the number of services needed and adjust as needed.
[4] FedRAMP, *Creating Effective Cloud-Computing Contracts for the Federal Government: Best Practices for Acquiring IT as a Service* (February 24, 2012)
[5] OMB Circular No. A-130, *Managing Information as a Strategic Resource* (July 2016)

services and contracts, it is challenging to manage resources effectively, leading to increased security risks and potential data mismanagement.

We identified findings related to this best practice in five OIG reports. For example, in 2015 the Department of Defense (DOD) OIG found that the DOD did not maintain a comprehensive list of cloud computing service contracts.[6] As a result, DOD could not determine whether it achieved actual cost savings or benefits from adopting cloud computing services. In addition, without knowing what data DOD Components place on the cloud, the DOD may not effectively identify and monitor cloud computing security risks. The USPS OIG also found this to be an issue. In its 2014 audit of the agency's management of cloud computing contracts and environment, the USPS OIG found that the Postal Service did not have an enterprise-wide inventory of cloud computing services.[7] As a result, the Postal Service could not effectively manage its cloud computing technologies and ensure the accountability and security of those technologies.

In another example, in 2024 the DOI OIG found that the Department did not have a complete inventory of its cloud-based systems and did not ensure they were purchased using procurement contracts from FedRAMP-approved CSPs.[8] The DOI OIG also found similar concerns related to an inaccurate inventory in its May 2015 inspection of the Department's adoption of cloud computing technologies.[9] This leads to a variety of potential problems. Information systems that are not included in the Department's inventory are not visible to the CIO, who is responsible for ensuring the security of all information systems that Department employees and contractors use on behalf of the Government. Also, cloud-computing systems not included in the Department's inventory do not undergo the Department's information security accreditation and authorization process. 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. Additionally, if the purchases are made via a CSP's default service contract instead of an approved procurement contract, the CSP may be able to unilaterally modify contract terms and potentially put Department data stored in the cloud at increased risk of compromise.

1.2 Include Relevant Cloud Security Clauses in CSP Contracts

Agencies should ensure that contracts with CSPs include relevant cloud security clauses to ensure cloud services are secure and that CSPs perform necessary security activities, such as security control assessments, for cloud-based information systems. Agencies should also ensure that their procurement guidance integrates Federal requirements and includes the Federal Risk and Authorization Management Program (FedRAMP)[10] recommended contract clauses for contracts with CSPs. As a best practice,

---

[6] DOD OIG Report No. DODIG-2016-038, *DOD Needs an Effective Process to Identify Cloud Computing Service Contracts* (December 28, 2015)

[7] USPS OIG Report No. IT-AR-14-009, *Management of Cloud Computing Contracts and Environment* (September 4, 2014)

[8] DOI OIG Report No. 2022-ITA-025, *The U.S. Department of the Interior Needs to Better Protect Data Stored in the Cloud from the Risk of Unauthorized Access* (February 21, 2024)

[9] DOI OIG Report No. ISDN-EV-OCI-0002-2014, *U.S. Department of the Interior's Adoption of Cloud Computing Technologies* (May 21, 2015)

[10] FedRAMP was established in 2011 to provide a cost-effective, risk-based approach for the adoption and use of cloud services by the federal government. In December 2022, the FedRAMP Authorization Act was signed as part of the Fiscal Year 2023 National Defense Authorization Act (NDAA) which codifies the FedRAMP program as the

FedRAMP recommends contracts with cloud service providers include 12 clauses that address security controls. The clauses address controls areas such as those that govern data jurisdiction, provide for boundary protection, protect against unauthorized access and disclosure of information, and ensure appropriate record retention and accountability for digital signatures.[11] If required provisions are not included in contracts, agencies may be at an increased risk of potential exposure or security breaches, and may not have a contractual remedy from the supplier if there is unauthorized use, modification or disclosure of their information.

We identified findings related to this best practice in 10 OIG and GAO reports. For example, in its 2023 audit of the Department of Transportation's (DOT) cloud-based systems' security, the DOT OIG found that although the Department reported it used standard cloud clauses in contracts for CSP services, not all of the contracts reviewed included the required security clause language.[12] Without the required security clause language, agency security officials could not ensure that the CSP would perform the necessary security activities, such as security control assessments for cloud-based information systems. Similarly, in its 2017 audit of the security of the National Aeronautics and Space Administration's (NASA) cloud computing services, the NASA OIG found that contracts and agreements were missing one or more critical provisions aimed at ensuring appropriate security over and access to the NASA data stored in the cloud.[13]

The U.S. Postal Service (USPS) OIG audited the Postal Service's cloud computing contracts and environment in 2014 and found that because the Postal Service did not include required information security clauses, the cloud computing environment may be at increased risk of unauthorized access, use, disclosure, and modification.[14] The OIG also found that without the required information security clause that requires the provider to cooperate with the agency to identify the sensitivity and criticality of the application, determine and comply with information security requirements and mitigate all security vulnerabilities identified during site security reviews, the Postal Service's data may be at increased risk of potential exposure and security breach.

In another review of cloud computing contracts and policy in 2014, the USPS OIG found that the Postal Service did not include adequate language to address information accessibility and data security for network access and server locations.[15] Specifically, the Postal Service did not require CSPs to state the amount of access they should have to the agency's data and information network. Management also did not include contract requirements to allow for the OIG to have real-time monitoring capability and network access. Additionally, in one contract, the Postal Service did not include contract language to address incident responsiveness, restricted access, vendor indemnification and cloud data ownership. Including contract language to address these findings would help prevent system breaches and data leaks and ensure access to information needed for investigations.

---

authoritative standardized approach to security assessment and authorization for cloud computing products and services that process unclassified federal information.

[11] FedRAMP, *Control Specific Contract Clauses*, V2.0 (June 6, 2014)

[12] DOT OIG Report No. IT2023043, *DOT's Cloud-Based Systems' Security Weaknesses Hinder Its Transition to a Zero Trust Architecture* (August 30, 2023)

[13] NASA OIG Report No. IG-17-010, *Security of NASA's Cloud Computing Services* (February 7, 2017)

[14] USPS OIG Report No. IT-AR-14-009, *Management of Cloud Computing Contracts and Environment* (September 4, 2014)

[15] USPS OIG Report No. SM-MA-14-005, *Cloud Computing Contract Clauses* (April 30, 2014)

Further, within a 2022 Federal agency cross-cutting GAO report on Cloud Computing, the GAO identified procuring cloud services as a challenge to Federal agencies and identified that an important part of procuring cloud services is incorporating a service level agreement into the contract.[16] Specifically, they identified that agencies did not always specify what constitutes a security breach and the responsibilities for notifying the agency, how data and networks will be managed and the range of enforceable consequences for non-compliance with the agreement.

1.3 Monitor CSP Performance and Include Enforcement Mechanisms in CSP contracts.

Agencies should adequately monitor applications, to include receiving and reviewing availability reports, to ensure CSPs achieve agreed upon service levels. They should also ensure contracts with CSPs include enforcement mechanisms that prescribe penalties when service levels are not met. As a best practice, the Federal CIO and Chief Acquisition Officer Councils recommend contracts for cloud services clearly define how performance is guaranteed – such as response time, resolution or mitigation time, and availability – and require providers to monitor their service levels and provide timely reporting of failures to meet service levels. Agencies that do not adequately monitor applications to ensure CSPs meet contract terms may not recognize that suppliers have experienced outages or failed to meet uptime percentages, and therefore, may not realize they are due service credits. This also increases the risk of public funds being misspent by paying for a level of service that a CSP has not met. Additionally, critical agency information may be at risk when agencies do not effectively monitor CSP performance to ensure information security requirements are followed.

We identified findings related to this best practice in four OIG reports. For example, in the previously mentioned 2014 USPS OIG audit of cloud computing contracts and environment, the USPS OIG found that Postal Service management did not appropriately monitor applications to ensure system availability and uptime percentages were met as required by the contract.[17] As a result, they did not recognize applicable service credits based on the supplier's failure to meet performance requirements. Similarly, in its 2024 evaluation of the Department of Interior's (DOI) cloud computing controls, the OIG found that none of the contracts reviewed during the evaluation included enforcement mechanisms that prescribed penalties for failure to meet agreed-upon service levels.[18] As a result, the Department had no assurance that respective CSPs met required service levels.

In a 2015 software contract and compliance review across the Postal Service organization, the USPS OIG found that the Postal Service did not effectively monitor performance to ensure the supplier followed all information security requirements as required by the contract, putting sensitive and critical information at risk.[19] The Department of Health and Human Services (HHS) OIG had similar findings in 2019 when auditing a National Institutes of Health (NIH) cloud program.[20] Specifically, the OIG found that the NIH did not adequately monitor whether the CSP had implemented adequate security controls to protect

---

[16] GAO Report No. GAO-22-106195, *Cloud Computing: Federal Agencies Face Four Challenges* (September 2022)
[17] USPS OIG Report No. IT-AR-14-009, *Management of Cloud Computing Contracts and Environment* (September 4, 2014)
[18] DOI OIG Report No. 2022-ITA-025, *The U.S. Department of the Interior Needs to Better Protect Data Stored in the Cloud from the Risk of Unauthorized Access* (February 21, 2024)
[19] USPS OIG Report No. IT-AR-15-009, *Software Contract and Compliance Review* (September 18, 2015)
[20] HHS OIG Report No. A-18-17-09304, *The National Institutes of Health Could Improve Its Monitoring to Ensure That an Awardee of the All of Us Research Program Had Adequate Cybersecurity Controls to Protect Participants' Sensitive Data* (June 2019)

sensitive data, and in its testing, the OIG found vulnerabilities that could potentially expose personally identifiable information, including personal health information.

Theme 2: Agencies Must Protect and Monitor Their Data

Data is not only an operational asset, but a national resource. The protection of this data is paramount to national security, public trust, and the effective functioning of government agencies. Data protection refers to security strategies and processes that help secure sensitive information from corruption, compromise, or loss. While operating in the cloud, data protection is critical due to the shared responsibility model, where both the cloud service provider and the user have roles in maintaining security. Additionally, Federal agencies may not have full control over their data as it is no longer housed in dedicated data centers but distributed across various locations.

The strategies for data protection must be multifaceted, involving legal, technical and administrative measures. A critical first step is knowing what data you have and where it resides, necessitating a thorough data inventory and cataloging process. This foundation is crucial for implementing best practices in data protection.

Guidance from the CIO Council and the Office of Management and Budget (OMB) emphasize the importance of robust data protection policies to prevent the breach or misuse of government data, which can lead to significant repercussions, including but not limited to, the compromise of classified information, financial loss and erosion of public confidence.[21] The Federal Chief Data Officers (CDO) Council recommends data inventories as the foundation to any formal data management program and suggests that data inventories aid in efficiently finding, accessing, and using data assets.[22] OMB's guidance on data inventories is that agencies should develop and maintain a comprehensive data inventory that accounts for all data assets created, collected, controlled or maintained by the agency.[23] In addition, agencies should only use approved cloud services to store agency data and implement mechanisms to protect PII and CUI data from unauthorized disclosure.

Of the 35 reports the working group analyzed, 15 had findings related to data protection and monitoring practices.

Recommended Best Practices:

2. We recommend that Federal agencies implement the following best practices to have more effective protection and monitoring controls for agency data that resides in the cloud:
   2.1 Establish and maintain an accurate data inventory.
   2.2 Use approved cloud services to store and share data.
   2.3 Protect PII and CUI data from unauthorized disclosure.

[21] OMB Memorandum No. M-16-04, *Cybersecurity Strategy Implementation Plan for the Federal Civilian Government* (August 2015)
[22] Federal CDO Council, *Enterprise Data Inventories* (April 2022)
[23] Supplemental Guidance on the Implementation of OMB Memorandum No. M-13-13, *Open Data Policy—Managing Information as an Asset* (May 2013)

2.1 Establish and Maintain an Accurate Data Inventory

Agencies should maintain an updated inventory of data locations and data classifications, while using appropriate storage solutions. This practice will help ensure that all data is properly stored and protected according to its level of sensitivity, which will allow for the application of appropriate security measures as per NIST and the Federal Information Security Modernization Act of 2014 (FISMA) guidelines.

We identified findings related to this best practice in three OIG reports. For example, in 2014 the USPS OIG found that the Postal Service did not address information accessibility and data security for network access and server locations in 13 cloud computing contracts.[24] In another 2015 USPS OIG report, it was discovered that the Postal Service did not know the location of emails and data.[25] As a result, federal systems and data could be at an increased risk for attack by malicious actors without having an awareness of systems and data and securing them properly.

In another example, in 2023 the Federal Deposit Insurance Corporation (FDIC) OIG found that the FDIC did not inventory data stored in the cloud environment or fully develop a data catalog.[26] Without complete visibility into what cloud data exists and where it resides, FDIC faced increased risks to security and privacy and overall effectiveness of operations.

2.2 Use Approved Cloud Services to Store and Share Data

Agencies should use whitelisted cloud services or a process for the evaluation and approval of new cloud services, while monitoring and preventing the use of unauthorized services. Unauthorized cloud services may not adhere to the policies, laws and regulations that are required by approved services. Without proper security like encryption and data loss prevention, unapproved cloud services may lead to inadequate control over data management, unauthorized data access, and legal penalties.

We identified findings related to this best practice in three OIG reports. Audits of NASA in 2017,[27] the Department of Energy (DOE) in 2023[28] and USPS in 2015[29] found the use of cloud services that were unapproved, lacked authorizations to operate, did not have system security plans or were not tested for adequate security controls. These services could have led to federal data becoming lost, stolen or destroyed, and could have allowed adversaries to breach federal networks.

2.3 Protect PII and CUI Data from Unauthorized Disclosure

Agencies should implement encryption for PII and CUI data at rest and in transit for cloud environments. In addition to effective implementation of encryption mechanisms, access controls should be implemented to restrict access to only authorized personnel, including access logging, access monitoring and secure disposal. Agencies should also train employees on the importance of handling sensitive information securely to prevent accidental disclosure. According to NIST, all moderate to high categorized systems are to be encrypted at rest, including CUI and PII data, and role-based access

[24] USPS OIG Report No. SM-MA-14-005, *Cloud Computing Contract Clauses* (April 30, 2014)
[25] USPS OIG Report No IT-AR-15-009, *Software Contract and Compliance Review* (September 18, 2015)
[26] FDIC OIG Report No. AUD-23-003, *The FDIC's Adoption of Cloud Computing Services* (July 2023)
[27] NASA OIG Report No. IG-17-010, *Security of NASA's Cloud Computing Services* (February 7, 2017)
[28] DOE OIG Report No. DOE-OIG-23-18, *Security Over Cloud Computing Technologies at Select Department of Energy Locations* (March 2023)
[29] USPS OIG Report No. IT-AR-15-009, *Software Contract and Compliance Review* (September 18, 2015)

control mechanisms should be implemented to govern who has access to data, based on their role.[30] NIST requires encryption for data at rest and in transit, security literacy training for new hires, periodically, and following specific events.

We identified findings related to this best practice in 10 OIG reports. In 2023, the Federal Housing Finance Agency (FHFA) OIG found that data at rest was not being encrypted and a single user was given privileged access for the system without the system owner's approval to the same system.[31] Lack of encryption increases the risk of unauthorized access and modification to data. An audit of HHS in 2019 also found a cloud-based system without adequate controls to protect PII, did not monitor the controls that protect PII and did not encrypt the locations that stored the data in the cloud.[32] Failing to adequately protect and secure PII data could result in unauthorized disclosure of PII.

Theme 3: Agencies Should Implement Effective Identity and Access Management Practices

Identity and Access Management (IAM) is a security and business discipline that includes multiple technologies and business processes to help the right people or machines to access the right assets at the right time for the right reasons. IAM is a cornerstone of an agency's information security posture that acts as the frontline defense against unauthorized access, data theft and security breaches. IAM cohesively integrates technologies, policies and procedures to manage identities through creation, requests for access, modification and termination.

The dynamic and distributed nature of cloud environments can offer challenges to effectively implementing IAM. These challenges can make consistent security controls difficult to maintain. IAM systems provide the necessary oversight and management tools to ensure that access policies are applied uniformly across all cloud resources. NIST guidance states that effective IAM practices in cloud environments are crucial to mitigating risks associated with unauthorized access.[33]

In cloud computing, security is a shared responsibility between the CSP and the customer. IAM helps agencies fulfill their responsibility to the CSP by ensuring that only authorized users can access cloud resources, in addition to continuously monitoring and managing access. To prevent identity-based attacks, agencies should implement multi-factor authentication (MFA) and role-based access controls. These defenses are critical methods of restricting network, system and file access based on the roles and status of those attempting to access them.

Of the 35 reports the working group analyzed, 12 had findings related to identity and access management practices.

---

[30] NIST SP 800-171 Rev. 3, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations* (May 2024)

[31] FHFA OIG Report No. AUD-2023-002, *FHFA Did Not Fully Implement Select Security Controls Over One of Its Cloud Systems as Required by NIST and FHFA Standards and Guidelines* (March 8, 2023)

[32] HHS OIG Report No. A-18-17-09304, *The National Institutes of Health Could Improve Its Monitoring to Ensure That an Awardee of the All of Us Research Program Had Adequate Cybersecurity Controls to Protect Participants' Sensitive Data* (June 2019)

[33] NIST SP 800-53 Rev. 5, *Security and Privacy Controls for Information Systems and Organizations* (September 2020)

Recommended Best Practices:

3. We recommend that Federal agencies implement the following best practices to have more effective identity and access management practices for managing access to agency resources in the cloud:
   3.1 Use a centralized identity and access management system.
   3.2 Enforce multi-factor authentication.
   3.3 Periodically audit user access privileges.
   3.4 Disable user access in a timely manner.
   3.5 Separate production and non-production environments.

3.1 Use a Centralized Identity and Access Management System

Agencies should use a centralized IAM system to assist in accurately requesting, authorizing, terminating and reviewing access to hardware, software and applications. IAM systems provide secure access to organizational resources such as email, databases, data and applications to verified entities. IAM systems can also help agencies employ multi-factor or two-factor authentication. By using a single access management platform across the agency, an agency can manage access in an effective, efficient, consistent and simplified manner.

The application of a robust IAM solution would have helped to mitigate findings identified within the two OIG reports related to this best practice. For example, the Treasury Inspector General for the Tax Administration (TIGTA) issued a report in 2022 which identified the lack of IAM as a weakness, placing taxpayer data at risk.[34] In this report, TIGTA stated that IAM "provides direction for all development activities for external authentication and authorization as well as technical integration and coordination of other public facing applications in support of the Information Technology organization's secure data access activities, both within the Internal Revenue Service (IRS) and with other Government agencies."

3.2 Enforce Multi-Factor Authentication

Agencies should enforce MFA on cloud-based systems to reduce the risk of unauthorized access. As Federal agencies move toward implementing Zero Trust Architecture[35] (ZTA), the OMB has issued guidance on enforcing MFA.[36] The application of MFA will harden agencies defenses against threat actors attempting to gain access to their networks even if passwords are compromised.[37] MFA adds layers of security by requiring users to provide two or more methods of identity verification to sign in, like a password or personal identification number combined with a personal identity verification (PIV) card, security token, or biometric factor.

We identified findings related to MFA in three OIG reports. In 2015, the Peace Corps OIG issued a report finding that the Peace Corps did not have two-factor authentication enabled for all users on a pilot cloud platform within its environment.[38] In 2023, the DOT OIG issued a report finding that the DOT had yet to

[34] TIGTA Report No. 2022-20-052, *Cloud Services Were Implemented Without Key Security Controls, Placing Taxpayer Data at Risk* (September 27, 2022)

[36] OMB Memorandum No. M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles* (January 26, 2022)
[37] Cybersecurity and Infrastructure Security Agency, *Multi-Factor Authentication* (January 2022)
[38] Peace Corps OIG No. IG-15-01-SR, *The Peace Corps' Cloud Computing Pilot Program* (March 17, 2015)

fully adopt MFA, stating that "implementation depends on successful allocation of funding."[39] In the same report, DOT OIG also found that applications did not use PIV cards for login. Without MFA and PIV cards, the security of the system relied solely on passwords, which can be weak, cracked, guessed and stolen. This results in increased risk of unauthorized access and data breaches, susceptibility to phishing attacks, weak access controls and non-compliance.

In the Department of Commerce's (DOC) OIG 2019 report on the Census Bureau's cloud security posture, auditors found that the Bureau's GovCloud root users' identification key and secret key, which function much like a username and password, were not being protected by MFA.[40] Not having MFA configured for the most privileged user accounts of the Bureau's GovCloud environments left the keys vulnerable to theft and misuse. The auditors later found that MFA was not supported for the GovCloud root user account to discourage the use of the account. Since MFA could not be implemented on the root user account, the Bureau should have disabled its GovCloud root user accounts to adhere to federal and Departmental requirements that privileged user accounts be configured to use MFA.

3.3 Periodically Audit User Access Privileges

Agencies should conduct periodic access reviews to ensure that only current authorized users have access, while auditing their privileges and adjusting them according to the principle of least privilege. The principle of least privilege, according to NIST, only allows access for users necessary to accomplish assigned tasks.[41] The application of least privilege will allow for agencies to detect unauthorized access, identify insider threats and improve the transparency and accountability of users. Failing to regularly review access lists may result in accumulated excess of permissions, which violates the principle of least privilege but could also lead to misuse, unauthorized entry, data theft or sabotage.

We identified findings related to periodic review of user access privileges in seven reports. For example, in 2015 the USPS OIG found that administrators were not terminating access to software for users that no longer needed it.[42] The FHFA OIG also identified this issue in 2023 as there was a user given privileged access without system owner's approval.[43] In four other reports, OIGs found that the administrators were not reviewing the access listings. Failing to regularly review user access lists and privileges will cause an accumulation of excessive and unnecessary privileges and access points, increased risk of insider threats and unauthorized access, greater vulnerability to security breaches and a lack of accountability which will negatively affect the Incident Response team.

3.4 Disable User Access in a Timely Manner

Agencies should automatically disable accounts that have been inactive for a set period to reduce the risk of dormant accounts being compromised and used. The typical time used for this dormant period is

[39] DOT OIG Report No. IT2023043, *DOT's Cloud-Based Systems' Security Weaknesses Hinder Its Transition to a Zero Trust Architecture* (August 30, 2023)
[40] DOC OIG Report No. OIG-19-015-A, *The Census Bureau Must Correct Fundamental Cloud Security Deficiencies in Order to Better Safeguard the 2020 Decennial Census* (June 19, 2019)
[41] NIST SP 800-53 Rev. 5, *Security and Privacy Controls for Information Systems and Organizations* (September 2020)
[42] USPS OIG Report No. IT-AR-15-009, *Software Contract and Compliance Review* (September 18, 2015)
[43] FHFA OIG Report No. AUD-2023-002, *FHFA Did Not Fully Implement Select Security Controls Over One of Its Cloud Systems as Required by NIST and FHFA Standards and Guidelines* (March 8, 2023)

30-90 days. The Center for Internet Security suggests 45 days.[44] This practice helps to prevent unauthorized access and insider threats.

We identified five reports with findings related to disabling user access in a timely manner. For example, in the 2023 audit report from the DOT OIG, the OIG recommended the implementation of a process to automatically disable user accounts after 60 days of inactivity.[45] The 2015 USPS audit found that 82 percent of accounts had not accessed information resources in 90 days yet remained with privileges to do so.[46] The audit's recommendation was that administrators follow agency policy which states that user access must be audited semiannually and accounts that have been dormant for 90 days must be disabled. In addition, in 2023 the TIGTA OIG also found that user accounts on the Enterprise Case Management system were not deactivated or disabled timely, potentially allowing unauthorized access to taxpayer data and privacy information.[47]

3.5 Separate Production and Non-production Cloud Environments

Agencies should maintain a strict separation between production and non-production environments, while ensuring that vendor, test accounts and shared accounts are not being used in production and are monitored closely. This practice will serve a multitude of purposes: (1) protect the stability and performance of critical services in production environments, (2) ensure that sensitive production data is not accessible through less secure environments or accounts, (3) minimize the possibility of security incidents and insider threats and (4) maintain the accountability and auditability of the system by the preventing anonymous changes from shared, test or vender accounts.

We identified three reports related to this best practice. The USPS OIG found in 2015 that there were two shared accounts in use during their audit, but these have been deactivated since.[48] A report from the Export-Import Bank (EXIM) OIG in 2017 identified that EXIM also had identified findings with the implementation of shared accounts.[49] A report from the Social Security Administration's OIG in 2019 also recommended assessing the risk of cloud service provider root accounts and restricting global administrator accounts.[50]

Theme 4: Agencies Should Implement Effective Configuration Management Practices

NIST requires agencies to adopt structured approaches to maintaining system integrity and security by creating robust configuration management practices.[51] Configuration management is the process of ensuring that the configurations of a system's servers, applications and other environments remain known, consistent and trusted over time. Configuration management is crucial for Federal agencies

---

[44] Center for Internet Security, *CIS Critical Security Controls v8, 5.3: Disable Dormant Accounts* (2021)
[45] DOT OIG Report No. IT2023043, *DOT's Cloud-Based Systems' Security Weaknesses Hinder Its Transition to a Zero Trust Architecture* (August 30, 2023)
[46] USPS OIG Report No. IT-AR-15-009, *Software Contract and Compliance Review* (September 18, 2015)
[47] TIGTA Report No. 2023-20-018, *The Enterprise Case Management System Did Not Consistently Meet Cloud Security Requirements* (March 27, 2023)
[48] USPS OIG Report No. IT-AR-15-009, *Software Contract and Compliance Review* (September 18, 2015)
[49] EXIM OIG Report No. OIG-AR-17-04, *Independent Audit of Export-Import Bank's Information Security Program Effectiveness for Fiscal Year 2016* (March 15, 2017)
[50] Social Security Administration OIG Report No. A-14-18-50498, *Security of the Social Security Administration's Cloud Environment* (August 2019)
[51] NIST SP 800-123, *Guide for Security-Focused Configuration Management of Information Systems* (October 2019)

operating in the cloud because it ensures consistency, security and compliance across dynamic cloud environments. Effective configuration management requires a detailed record of all system components and their configurations within an organization, including tracking all hardware, software, and network settings to ensure security and compliance by systematically identifying, controlling, and documenting changes to these configurations. Without effective configuration management controls in place, the risk of unauthorized access, data breaches and non-compliance with federal regulations increases. In addition, given the nature of cloud environments being rapidly scalable where virtual resources can be deployed quickly, without configuration management controls in place, unmanaged changes to one virtual resource could propagate unintended consequences across the entire infrastructure.

Effective implementation of configuration management controls has multiple benefits including, enhanced security, operational efficiency, risk management and cost optimization. If resources are controlled appropriately, agencies can monitor and optimize resource usage in the cloud and avoid over-provisioning of resources to help manage cloud costs. In addition, effectively implementing these controls allows agencies to remain compliant with federal regulations and standards such as FedRAMP and FISMA.

Of the 35 reports the working group analyzed, 11 had findings related to configuration management practices.

Recommended Best Practices:

4. We recommend that Federal agencies implement the following best practices to have more effective configuration management practices for managing changes to agency resources in the cloud:
   4.1 Establish and maintain baseline configurations.
   4.2 Establish and maintain a complete and accurate asset inventory.

4.1 Establish and Maintain Baseline Configurations

Agencies should establish and maintain baseline configurations for all cloud-based systems. This is a frequent practice to secure both cloud-based and on-premises systems. Without baseline configurations established, cloud systems can be misconfigured or configured in a manner that is not in accordance with established CSP standards or best practices. This can allow for unauthorized access to systems and data. A 2023 DOT OIG report found weaknesses in seven of DOT's systems, including weaknesses involving configuration management.[52] Specifically, there was a lack of security baseline configuration settings and checklists that introduces risks to network security due to a lack of visibility into software packages installed on servers, network components and security patch software update information on the operating system and applications.

Maintaining configuration baselines is also integral to secure cloud-based systems. Agencies should have an established process to periodically perform baseline configuration reviews of configuration settings for cloud-based systems. Unauthorized and unmanaged changes to configuration settings that could lead to vulnerabilities on systems such as exposing data to unauthorized users. Additionally, outdated configuration practices should be reviewed and updated to ensure they are up to date in line with the latest security best practices. A 2023 FHFA OIG report found that the agency did not perform periodic

[52] DOT OIG Report No. IT2023043, *DOT's Cloud-Based Systems' Security Weaknesses Hinder Its Transition to a Zero Trust Architecture* (August 2023)

configuration baseline reviews of configuration settings.[53] Specifically, FHFA did not perform monthly configuration compliance scans required by internal agency standards and guidelines, increasing the likelihood that deviations from approved baseline configurations were not being detected and corrected.

The DOC OIG found in 2019 that system administrators had not fully implemented cloud security baselines, which led to a weakened and vulnerable security posture of the cloud environment.[54] This issue should have been identified through Information Security assessments; however, the assessments were not performed or when performed, were insufficient. For example, the assessments indicated the cloud environment baselines had been implemented when they had not. This could allow security vulnerabilities to persist with no awareness of the weaknesses.

4.2 Establish and Maintain a Complete and Accurate Asset Inventory

Agencies should establish and maintain an inventory of all system components connected to cloud-based systems. NIST defines an information system component as "[a] discrete, identifiable information technology asset (e.g., hardware, software and firmware) that represents a building block of an information system.[55] The components involve interfaces, storages, computing power or networks. The lack of inventory for all components connected to cloud-based systems could allow for unknown and unmanaged interfaces or connections. This can lead to unauthorized usage of systems and data. Agencies must define the basic information to be collected, such as hardware specifications, software license information, software version numbers and component owners. This inventory should also be reviewed and updated regularly. The same 2023 FHFA OIG report found that FHFA did not develop a component inventory for its cloud system as required by NIST SP 800-128.[56] As a result, FHFA risked not knowing which computing resources were connected to or within the boundary of its cloud system.

More broadly, agencies should implement and maintain a complete and accurate inventory of all cloud-based systems. Having an inventory of all cloud-based systems is important to secure data within systems. Data cannot be secured in a system the agency does not have knowledge about. This can also lead to ineffective responses to incidents if a breach occurs. Five OIGs found instances where their agency lacked a complete and accurate inventory of cloud-based systems. This includes DOE, USPS, NASA, Department of Veterans Affairs (VA), and the Board of Governors of the Federal Reserve System (FRB).

At the DOE, in 2023 the OIG reported that DOE did not maintain an accurate inventory of cloud-based systems used across the enterprise, and programs and sites generally used more systems than were reported to the Office of the Chief Information Officer.[57] USPS OIG in 2014 found that Postal Service did

[53] FHFA OIG Report No. AUD-2023-002, *FHFA Did Not Fully Implement Select Security Controls Over One of Its Cloud Systems as Required by NIST and FHFA Standards and Guidelines* (March 2023)
[54] DOC OIG Report No. OIG-19-015-A, *The Census Bureau Must Correct Fundamental Cloud Security Deficiencies in Order to Better Safeguard the 2020 Decennial Census* (June 19, 2019)
[55] NIST SP 800-53 Rev. 5, *Security and Privacy Controls for Information Systems and Organizations* (September 2020)
[56] FHFA OIG Report No. AUD-2023-002, *FHFA Did Not Fully Implement Select Security Controls Over One of Its Cloud Systems as Required by NIST and FHFA Standards and Guidelines* (March 2023)
[57] DOE OIG Report No. DOE-OIG-23-18, *Security Over Cloud Computing Technologies at Select Department of Energy Locations* (March 2023)

not establish an enterprise-wide inventory of cloud computing services.[58] Specifically, at that time Postal Service did not include the name of the service, CSP, deployment model, service model and contract number, as required by internal policy. The Postal Service attributed the cause to not having a single group responsible for managing cloud services, including developing and maintaining an inventory of all cloud services. The NASA OIG discovered in 2017 that the agency had an additional 20 cloud services in use that were not approved.[59] In addition, in 2023 the VA OIG identified 37 devices that were using software not authorized.[60] These became part of the agencies "shadow IT" or IT on an agency's network that the CIO or CISO did not purchase or authorize for use. The FRB OIG found in 2022 that the Federal Reserve Board Cloud Resource Center's inventory of cloud systems was incomplete.[61] A key reason for omissions was that the Cloud Resource Center issued guidance on its cloud inventory processes in 2020, and it had not fully accounted for division cloud systems purchased before 2020.

Theme 5: Agencies Should Implement Effective Continuous Monitoring Controls

Continuous monitoring is a process of ongoing awareness of information security, threats and vulnerabilities to facilitate risk-based decision making. Ongoing monitoring of organizational security architecture and accompanying security programs is a critical part of the risk management process to ensure that organization-wide operations remain within an acceptable level of risk to the organization, despite changes that occur. It is also an important tool for agencies to monitor compliance issues and to help manage risks and assist in decision making. Without continuous monitoring, decision makers may have limited to no assurance that controls are in place and working, and an increased risk that vulnerabilities are not identified in a timely manner. NIST guidance requires Federal agencies to implement continuous monitoring controls for information security including providing ongoing awareness, allowing for controlling risk in highly dynamic environments, allowing for effective and timely risk-based decisions and being more efficient with automated tools.[62] This requirement still exists even when the agency utilizes Cloud platforms and applications.

Agencies should develop and implement a plan for continuous monitoring for security controls that are the responsibility of the agency which will vary depending on the shared responsibility model and assessed NIST Federal Information Processing Standards (FIPS) Publication 199 system risk categorization level for each cloud-based system.[63] FIPS 199 requires Federal agencies to assess their information systems in each of the confidentiality, integrity, and availability categories, rating each system as low, moderate or high impact and determining the overall security categorization for systems. A system's category is dependent on the potential impact on an agency's assets and operations should their information systems be compromised through unauthorized access, use, disclosure, disruption, modification or destruction. These are the standards CSPs must employ to ensure their services meet

[58] USPS OIG Report No. IT-AR-14-009, *Management of Cloud Computing Contracts and Environment* (September 2014)
[59] NASA OIG Report No. IG-17-010, *Security of NASA's Cloud Computing Services* (February 2017)
[60] VA OIG Report No. 22-02961-71, *Inspection of Information Security at the St. Cloud VA Medical Center in Minnesota* (June 2023)
[61] FRB OIG Report No. 2022-IT-B-006, *The Board Can Strengthen Inventory and Cybersecurity Life Cycle Processes for Cloud Systems* (March 2022)
[62] NIST SP 800-53 Rev. 5, *Security and Privacy Controls for Information Systems and Organizations* (September 2020)
[63] NIST FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems* (February 2004)

the minimum-security requirements for the data processed, stored and transmitted. These impact levels ensure that systems have the appropriate security controls to manage their relevant risks, safeguarding sensitive information. The shared-responsibility model dictates that the CSP must monitor and respond to security threats related to the cloud itself and its underlying infrastructure. However, the notion of shared responsibility can be misunderstood. This leads to the assumption by the customer (agency) that their cloud environment and any applications, data or activity associated with them – are fully protected by the cloud provider. Agencies themselves must also perform periodic reviews of continuous monitoring reports provided by the cloud provider that should indicate the implementation status of security controls, deficiencies identified and time-bound plans to remediate those weaknesses. Under FedRAMP, each Federal agency that issues an Authority to Operate (ATO) for a Cloud Service Offering (CSO) is responsible for reviewing the CSP's continuous monitoring activities to ensure the security posture remains sufficient for its own use and supports an ongoing authorization.[64] This includes reviewing the monthly plan of action and milestones (POA&M), approving deviation requests or significant changes to the platform or application, and reviewing the results of the annual assessment of security and privacy controls.

Of the 35 reports that the working group analyzed, 10 had findings related to the continuous monitoring process for cloud-based systems.

Recommended Best Practices:

5. We recommend that federal agencies implement the following best practices to have more effective continuous monitoring practices for ongoing awareness of information security, vulnerabilities, and threats to support risk management decisions for cloud-based systems:
   5.1 Prioritize continuous monitoring and establish and implement a continuous monitoring process.
   5.2 Ensure all security artifacts are maintained and use all available information to perform continuous monitoring.
   5.3 Take appropriate actions in response to continuous monitoring findings.

5.1 Prioritize Continuous Monitoring and Establish and Implement a Continuous Monitoring Process

FISMA requires Federal agencies to implement continuous monitoring of FISMA accredited systems. Additionally, NIST standards require continuous monitoring to control risk in a dynamic environment and to allow for effective and timely risk-based decisions.[65] We identified three reports related to this best practice. The GAO cites that developing and implementing a plan for continuously monitoring the cloud system is a key practice that agencies should follow.[66] These key practices include developing and implementing a plan for continuously monitoring the security controls that are the agency's responsibility, reviewing continuous monitoring deliverables from the CSP, documenting the use of vulnerability management procedures and tools to monitor the agency's cloud infrastructure and collecting and reviewing audit logs.

[64] General Services Administration, *FedRAMP Agency Authorization Playbook* (February 2024)
[65] NIST SP 800-53 Rev. 5, *Security and Privacy Controls for Information Systems and Organizations* (September 2020)
[66] GAO Report No. GAO-23-105482, *Cloud Security: Selected Agencies Need to Fully Implement Key Practices* (May 2023)

The 2023 GAO report found that agencies partially implemented continuous monitoring. In some cases, they developed a plan, but did not implement it or did not fully implement it. Additionally, in 2023 the VA OIG found that management lacked assurance that security controls were operating effectively due to the lack of continuous monitoring.[67] The VA OIG audit team found that some systems did not have all documented contingency, incident response or disaster plans; three systems were missing at least one plan. The VA OIG found that 9 of 13 selected systems were missing the required documentation. As a result, they found that security controls may not be operating effectively or implemented correctly and could result in increased security risks allowing for unauthorized access to systems and data. The VA OIG found that their agency must improve its oversight of continuous monitoring to ensure they are protected. The DOL OIG found in 2022 that DOL was not always completing its continuous monitoring reviews of CSPs and corresponding checklists at the required frequency per DOL policies.[68] In addition, a 2022 TIGTA OIG audit found that the IRS was not conducting required FedRAMP security reviews for continuous monitoring for a cloud platform within the IRS environment.[69] Failure to conduct the third-party continuous monitoring checklist could lead to an increase in undetected security risks, which could result in a compromise of the integrity, confidentiality and security of the agency's information systems.

5.2 Ensure All Security Artifacts Are Maintained and Use all Available Information to Perform Continuous Monitoring

Agencies should consider all identified risks when granting authority to operate cloud systems. These risks usually document the security posture of the cloud system and what existing weaknesses there are in selected control families. When risk information is available to agencies from third party assessments, POA&Ms, or other documents, these risks should be evaluated before granting authority to operate. Identified risks provide valuable insights when choosing a cloud vendor as that will affect the agency's internal continuous monitoring regarding the system and documenting how much risk the agency will take on.

We identified two reports related to this best practice, including one that found that the agency did not use all available information. The DOD OIG found in 2023 that the DOD used three commercial CSOs that were FedRAMP and DOD authorized for the systems reviewed.[70] However, the authorizing officials did not review all required documentation to consider the authorized commercial CSOs' risks to their systems when granting and reassessing the authority to operate on a periodic basis thereafter. Here, the authorizing officials did not consider all available risks because they thought that the FedRAMP and DOD authorizations were sufficient. As a result, they may be unaware of all vulnerabilities and cyber security risks.

However, to do so, agencies need to ensure security artifacts are properly maintained. The same 2023 GAO report above found that agencies could not conduct continuous monitoring because security artifacts were not maintained. As a result, this resulted in excess costs to correct the vulnerabilities.[71]

---

[67] VA OIG Report No. 22-03525-195, *VA Should Strengthen Enterprise Cloud Security and Privacy Controls* (September 27, 2023)

[68] DOL OIG Report No. 23-22-001-07-725, *FY 2021 FISMA DOL Information Security Report: Information Security Continuous Monitoring Controls Remain Deficient* (January 28, 2022)

[69] TIGTA OIG Report No. 2022-20-051, *Taxpayer Digital Communications Platform Security and Access Controls Need to be Strengthened* (September 21, 2022)

[70] DOD OIG Report 2023-052, *Audit of the DOD's Compliance with Security Requirements When Using Commercial Cloud Services* (February 15, 2023)

[71] GAO Report No. GAO-23-105482, *Cloud Security: Selected Agencies Need to Fully Implement Key Practices* (May 2023)

Agencies must ensure that all security artifacts are maintained to ensure that all available information is readily available for the agency to perform continuous monitoring.

5.3 Take Appropriate Actions in Response to Continuous Monitoring Findings

Agencies should take appropriate actions in response to any risks identified during the continuous monitoring process. Agencies should ensure POA&Ms for information systems are developed and updated in a timely manner to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the security controls assessment and to reduce or eliminate known vulnerabilities. Additionally, the POA&Ms for information systems should be developed and updated in a timely manner to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during any security controls assessment.

In one 2022 audit, TIGTA found that the agency did not meet guidelines for the timely creation and documentation of POA&Ms to address security risks identified.[72] Also, they did not remediate cloud security vulnerabilities identified from a vulnerability scan in required times. The internal policies required creating POA&Ms for critical and high-risk vulnerabilities that cannot be remediated in 30 or 60 days, respectively. Without a sound remediation process and without documenting POA&Ms, the IRS cannot ensure that it is correcting security weaknesses and may not effectively remediate vulnerabilities. TIGTA had similar findings on the creation and implementation of POA&Ms for remedial actions in two other 2023 audits.[73]

Theme 6: Agencies Should Implement Effective Assessment and Authorization Practices

The assessment and authorization (A&A) process is key for Federal agencies that operate their systems in the cloud, as it ensures that systems and services comply with stringent security and compliance standards. The A&A process requires that designated security controls based on system risk level are assessed for effectiveness and compliance prior to authorization to go live. These processes must be updated and maintained as a cyclical practice. A&A forms the foundation of a risk management strategy for Federal agencies. To support the overall IT risk management strategy for Federal agencies, the process systematically assesses risk, implements necessary controls to mitigate risk and gets formal approval from an authority that understands the potential impact. This authorization process for cloud-based systems that support the Federal government is guided by the FedRAMP program, FISMA and NIST standards.[74]

In cloud environments, the distributed nature and shared responsibility of security between the cloud service provider and customer makes it imperative that Federal customers of cloud services must follow the A&A process rigorously to ensure complete and effective security control coverage. By not assessing security controls to perform security accreditations and authorizations as mandated, Federal agencies expose themselves to significant risks including increased exposure to threats such as data breaches,

---

[72] TIGTA Report No. 2022-20-065, *The IRS Needs to Improve Its Database Vulnerability Scanning and Patching Controls* (September 2022)

[73] TIGTA Report No. 2023-20-018, *The Enterprise Case Management System Did Not Consistently Meet Cloud Security Requirements* (March 27, 2023) and Report No. 2023-20-013, *The IRS Implemented the Business Entitlement Access Request System; However, Improvements Are Needed* (March 22, 2023)

[74] NIST SP 800-37, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy* (December 2018)

ransomware and unauthorized access. In addition, the lack of awareness of security control posture for cloud-based systems can put sensitive data at risk of exposure or compromise.

Of the 35 reports the working group analyzed, 13 had findings related to assessment and authorization practices.

Recommended Best Practices:

6. We recommend that Federal agencies implement the following best practices to have more effective A&A practices to ensure that security controls are appropriately assessed and that cloud-based systems are operating at an acceptable level of risk to agencies:
   6.1 Perform security accreditations and authorizations.
   6.2 Develop and update the business impact assessment and system security plan.
   6.3 Fully Implement security controls, perform regular assessments and remediate flaws.

6.1 Perform Security Accreditations and Authorizations

Agencies that operate cloud-based systems should assess and attain security accreditations and authorizations such as FedRAMP authorization and ATO. By attaining and maintaining security accreditation, agencies demonstrate their commitment to securing sensitive data while avoiding potential penalties and legal issues related to non-compliance. Accreditation involves a comprehensive assessment of the system's security controls which can help bring potential security concerns to light and allow agencies to implement security measures to mitigate security risks.

We identified 11 reports related to this best practice. For example, in 2023 the DOD OIG found that the DOD was not following federal regulations and its own guidance when granting and maintaining ATOs.[75] The DOD did not ensure that its cloud service providers maintained an acceptable security posture by reviewing the required documents, such as an annual third-party security assessment, POA&Ms and monthly continuous monitoring reports, to consider risks when granting and reassessing the ATOs. NASA also did not follow federal regulations for cloud-based systems, as they did not complete the necessary steps to ensure that all approved cloud services were registered with FedRAMP and had proper ATOs.[76] The DOI also did not formally authorize systems for operations for three of its cloud-based systems.[77]

The VA OIG found in 2021 that the VA did not fully follow FedRAMP or VA policies for Software as a Service (SaaS) applications when it granted security authorizations and the authority to operate on the VA network for applications that lacked FedRAMP authorization.[78] By not meeting federal authorization requirements, the VA could not ensure that the security controls complied with federal standards and would adequately protect PII from unauthorized access.

6.2 Develop and Update the Business Impact Assessment and System Security Plan

Agencies should develop and maintain Business Impact Assessments (BIA) and System Security Plans (SSP). BIAs help to identify critical functions, assessment of risks, and inter-system/application

[75] DOD OIG Report No. DODIG-2023-052, *Audit of the DOD's Compliance with Security Requirements When Using Commercial Cloud Services* (February 15, 2023)

[76] NASA OIG Report No. IG-17-010, *Security of NASA's Cloud Computing Services* (7 February 2017)

[77] DOI OIG Report No. 2015-ITA-017, *Cloud Computing Security Documentation in the Cyber Security Assessment Management Solution* (November 2015)

[78] VA OIG Report No. 20-00426-02, *VA Applications Lacked Federal Authorizations, and Interfaces Did Not Meet Security Requirements* (December 2, 2021)

dependencies. SSPs help administrators' document security requirements, ensure the necessary controls are in place based on what the system is used for and allow for effective security assessments.

In 2019, the U.S. Securities and Exchange Commission (SEC) OIG recommended remediating the SEC's process for creating SSPs due to missing cloud-specific security controls.[79] In that audit, the SEC did not implement FedRAMP baseline controls required for cloud-based systems for which the SEC was responsible for as a cloud customer. As a result, the SEC could not adequately ensure compliance, assess risk, identify issues or mitigate vulnerabilities. In a 2017 NASA OIG audit, they identified that there were several cloud services where NASA did not have an SSP in place.[80] In addition, a 2014 USPS OIG audit found that, contrary to policy, administrators were failing to complete BIAs to identify the sensitivity and criticality of their applications.[81]

6.3 Fully Implement Security Controls, Perform Regular Assessments and Remediate Flaws

Agencies should fully implement security controls before deployment of cloud-based systems and periodically perform regular assessments of those security controls based on NIST standards. When the assessments uncover design or effectiveness issues within the controls, they should be remediated. This practice will ensure compliance with laws and regulations, including FISMA and NIST SP 800-53 and mitigate many risks involved with working in cloud-based environments. Federal agencies that operate in the cloud and their cloud service providers must implement the minimum required baseline of security controls as determined by the FIPS 199 security categorization for each cloud-based system to ensure that federal cloud-based systems have the appropriate security controls in place to manage risks and to safeguard sensitive information.

There were nine reports identified that were related to this best practice. In the same SEC report from 2019, the SEC OIG audit found that security assessment reports for SEC's cloud-based systems were incomplete. The security assessment reports did not include vulnerability information, the scope of FedRAMP information reviewed, and performed security assessments that did not match the SSPs and referenced outdated federal policies.[82] A 2022 DOC OIG audit identified that DOC did not incorporate the proper controls into their SSPs for high-value assets in the cloud.[83] Also, a 2023 DOE OIG audit revealed that in addition to not having proper approval nor conducting ATOs, systems were not being assessed for proper security controls.[84] In addition, a 2016 EXIM OIG audit found that the Bank did not implement all NIST controls for a cloud-based application and the applicable NIST 800-53 controls were not addressed by the third-party service provider.[85]

---

[79] SEC OIG Report No. 556, *The SEC Can More Strategically and Securely Plan, Manage, and Implement Cloud Computing Services* (November 7, 2019)
[80] NASA OIG Report No. IG-17-010, *Security of NASA's Cloud Computing Services* (7 February 2017)
[81] USPS OIG Report No. IT-AR-14-009, *Management of Cloud Computing Contracts and Environment* (4 September 2014)
[82] SEC OIG Report No. 556, *The SEC Can More Strategically and Securely Plan, Manage, and Implement Cloud Computing Services* (November 7, 2019)
[83] DOC OIG Report No. OIG-22-031-A, *Missing Security Controls Put the Department's Cloud-Based High Value Assets at Risk* (September 14, 2022)
[84] DOE OIG Report No. DOE-OIG-23-18, *Security Over Cloud Computing Technologies at Select Department of Energy Locations* (March 2023)
[85] EXIM OIG Report No. OIG-AR-16-02, *Independent Audit of Export-Import Bank's Information Security Program for Fiscal Year 2015* (February 2, 2016)

Scope and Methodology

As part of the CIGIE FAEC, Cross Cutting Issues Subcommittee[86] under the leadership of the Environmental Protection Agency (EPA) OIG Assistant Inspector General for Audit (AIGA) and the EXIM OIG AIGA, the FDIC OIG led a team of oversight personnel from four OIGs (DOI, FDIC, National Geospatial-Intelligence Agency and USPS) in conducting this review. The team performed the review from October 2023 through July 2024. in accordance with the CIGIE Quality Standards for Federal Offices of Inspector General (Silver Book). The work adheres to the professional standards of independence, due care and quality assurance, and the review team followed procedures to ensure the accuracy of the information presented.

The objective of our review was to identify best practices and lessons learned from past and current Federal oversight work performed related to cloud security to help guide Federal agencies to strengthen their overall security posture. To accomplish the review objective, the team searched CIGIE's Oversight.gov reports repository and the GAO website to identify government-wide oversight reports relevant to cloud security. Specifically, the team identified 35 oversight reports from 19 OIGs, and the GAO, issued between April 2014 and February 2024. The team reviewed the findings, conclusions and recommendations within the oversight reports and identified the overarching best practice themes in this report. This report is a compilation of the results of the OIG and GAO reports reviewed; the team performed no additional oversight work about the identified best practice themes.

See Appendix 2 for a complete list of federal oversight reports reviewed.

[86] The FAEC Cross-Cutting Issues Subcommittee supports the CIGIE Audit Committee's mission of leading or being involved in coordinated, government-wide activities that promote economy and efficiency in federal programs and operations and address areas of weakness and vulnerability with respect to fraud, waste, abuse and mismanagement.

Appendix 1 – Key Terms and Definitions

Authority to Operate (ATO)	An official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image or reputation), organizational assets, individuals, other organizations and the Nation based on the implementation of an agreed-upon set of security controls.
Cloud Computing	A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.
Cloud Service Model	There are many options when moving infrastructure, applications or services into the cloud. NIST has defined three basic cloud service models: Software-as-a Service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS). • SaaS: Consumers are users of the provider's applications running on an underlying cloud infrastructure. Applications are accessible via various client platforms. Consumers do not manage or control the underlying infrastructure. • PaaS: Consumers have the capability to deploy custom applications using provider-supplied languages, libraries, services and tools on the cloud infrastructure. Consumers do not manage or control the underlying infrastructure, but they have control over the deployed applications and potentially the configuration settings of the provider-supplied environment that is hosting the application. • IaaS: Consumers have the capability to provision computing resources to deploy and run environments and applications. Cloud providers manage the underlying infrastructure while the consumers have control over the computing resources, including some control of selected networking components (e.g., host-versus network-based firewall).
Cloud Service Provider (CSP)	An external company that provides a platform, infrastructure, applications and/or storage services for its clients.
Federal Risk and Authorization Management Program (FedRAMP)	The FedRAMP is a governmentwide program that provides a standardized approach to security assessment, authorization and continuous monitoring for cloud products and services.
Federal Information Security Modernization Act (FISMA)	Federal legislation that defines a framework of guidelines and security standards to protect government information and operations.

Least Privilege Principle	A design principle whereby each entity is granted the minimum system resources and authorizations that the entity needs to perform its function.
Service Level Agreement	A service contract that defines the specific responsibilities of the service provider and sets the customer's expectations.
Shared Responsibility Model	A model that outlines the different responsibilities between the customer and the CSP

Appendix 2 – Federal Oversight Reports Analyzed

The working group reviewed and analyzed 42 federal oversight reports related to cloud security from 19 OIGs and the GAO and identified common best practices within the 35 reports listed below:

Report No.	Title	Best Practice Themes					
		Oversight of CSPs	Data Protection and Monitoring	Identity and Access Management	Configuration Management	Continuous Monitoring	Assessment and Authorization
Department of Commerce OIG							
OIG-22-031-A	Missing Security Controls Put the Department's Cloud-based High Value Assets at Risk, 14 September 2022						X
OIG-19-015-A	The Census Bureau Must Correct Fundamental Cloud Security Deficiencies in Order to Better Safeguard the 2020 Decennial Census, 19 June 2019		X	X	X		
Department of Defense OIG							
DODIG-2023-052	Audit of the DOD's Compliance with Security Requirements When Using Commercial Cloud Services, 15 February 2023					X	X
DODIG-2016-038	DOD Needs an Effective Process to Identify Cloud Computing Service Contracts, 28 December 2015	X					
Department of Energy OIG							

Report No.	Title	Best Practice Themes					
		Oversight of CSPs	Data Protection and Monitoring	Identity and Access Management	Configuration Management	Continuous Monitoring	Assessment and Authorization
DOE-OIG-23-18	Security over Cloud Computing Technologies at Select Department of Energy Locations, 30 March 2023		X		X		X
Department of Health and Human Services OIG							
A-18-17-09304	The National institutes of Health Could Improve Its Monitoring to Ensure Than an Awardee of the *All of Us* Research Program had Adequate Cybersecurity Controls to Protect Participants' Sensitive Data, June 2019	X	X				
Department of the Interior OIG							
2022-ITA-025	The U.S. Department of the Interior Needs to Better Protect Data Stored in the Could from the Risk of Unauthorized Access, 21 February 2024	X					
2015-ITA-017	Cloud Computing Security Documentation in the Cyber Security Assessment Management Solution, 12 November 2015						X
ISDN-EV-OCI-0002-2014	U.S. Department of the Interior's Adoption of Cloud-Computing Technologies, 21 May 2015	X					
Department of Labor OIG							

Report No.	Title	Best Practice Themes					
		Oversight of CSPs	Data Protection and Monitoring	Identity and Access Management	Configuration Management	Continuous Monitoring	Assessment and Authorization
23-22-001-07-725	FY 2021 FISMA DOL Information Security Report: Information Security Continuous Monitoring Controls Remain Deficient, 28 January 2022		X			X	
Department of Transportation OIG							
IT2023043	DOT's Cloud-Based Systems' Security Weaknesses Hinder Its Transition to a Zero Trust Architecture, 30 August 2023	X	X	X	X		
Department of Veterans Affairs OIG							
22-03525-195	VA Should Strengthen Enterprise Cloud Security and Privacy Controls, 27 September 2023					X	
22-02961-71	Inspection of Information Security at the St. Cloud VA Medical Center in Minnesota, 8 June 2023		X	X	X		
20-00426-02	VA Applications Lacked Federal Authorizations, and Interfaces Did Not Meet Security Requirements, 2 December 2021						X
Export-Import Bank of the United States OIG							

Report No.	Title	Best Practice Themes					
		Oversight of CSPs	Data Protection and Monitoring	Identity and Access Management	Configuration Management	Continuous Monitoring	Assessment and Authorization
OIG-AR-18-04	Independent Audit of Export-Import Bank's Information Security Program Effectiveness for Fiscal Year 2017			X			
OIG-AR-17-04	Independent Audit of Export-Import Bank's Information Security Program for Fiscal Year 2016, 15 March 2017		X	X	X		
OIG-AR-16-02	Independent Audit of Export-Import Bank's Information Security Program for Fiscal Year 2015, 2 February 2016		X				X
Federal Deposit Insurance Corporation OIG							
AUD-23-003	The FDIC's Adoption of Cloud Computing Services, 25 July 2023		X		X		
Federal Housing Finance Agency OIG							
AUD-2023-002	FHFA Did Not Fully Implement Select Security Controls Over One of Its Cloud Systems as Required by NIST and FHFA Standards and Guidelines, 8 March 2023		X	X	X		
OIG for the Board of Governors of the Federal Reserve and the Consumer Financial Protection Bureau							
2022-IT-B-006	The Board Can Strengthen Inventory and Cybersecurity Life Cycle Processes for Cloud Systems, 23 March 2022				X	X	

Report No.	Title	Best Practice Themes					
		Oversight of CSPs	Data Protection and Monitoring	Identity and Access Management	Configuration Management	Continuous Monitoring	Assessment and Authorization
Government Accountability Office							
GAO-23-105482	Cloud Security: Selected Agencies Need to Fully Implement Key Practices, 18 May 2023					X	
GAO-22-106195	Cloud Computing: Federal Agencies Face Four Challenges, September 2022	X					
National Aeronautics and Space Administration OIG							
IG-17-010	Security of NASA's Cloud Computing Services, 7 February 2017	X	X		X		X
Peace Corps OIG							
IG-15-01-SR	The Peace Corps' Cloud Computing Pilot Program, 17 March 2015			X			X
Social Security Administration OIG							
A-14-18-50498	Security of the Social Security Administration's Cloud Environment, August 2019	X		X		X	X
Treasury Inspector General for Tax Administration							
2023-20-018	The Enterprise Case Management System Did Not Consistently Meet Cloud Security Requirements, 27 March 2023			X	X	X	X

Report No.	Title	Best Practice Themes					
		Oversight of CSPs	Data Protection and Monitoring	Identity and Access Management	Configuration Management	Continuous Monitoring	Assessment and Authorization
2023-20-013	The IRS Implemented the Business Entitlement Access Request System; However, Improvements are Needed, 22 March 2023					X	
2022-20-065	The IRS Needs to Improve its Database Vulnerability Scanning and Patching Controls, 30 September 2022		X			X	
2022-20-052	Cloud Services Were Implemented Without Key Security Controls, Placing Taxpayer Data at Risk, 27 September 2022			X			X
2022-20-051	Taxpayer Digital Communications Platform Security and Access Controls Need to be Strengthened, 21 September 2022			X		X	
U.S. Agency for International Development OIG							
A-000-15-006-P	Audit of USAID's Progress in Adopting Cloud Computing Technologies, 12 March 2015	X	X				
U.S. Postal Service OIG							
IT-AR-15-009	Software Contract and Compliance Review, 18 September 2015	X	X	X			

Report No.	Title	Best Practice Themes					
		Oversight of CSPs	Data Protection and Monitoring	Identity and Access Management	Configuration Management	Continuous Monitoring	Assessment and Authorization
IT-AR-14-009	Management of Cloud Computing Contracts and Environment, 4 September 2014	X			X		X
SM-MA-14-005	Cloud Computing Contract Clauses, 30 April 2014	X	X				
U.S. Securities and Exchange Commission OIG							
556	The SEC Can More Strategically and Securely Plan, Manage, and Implement Cloud Computing Services, 7 November 2019						X

Appendix 3 – Acronyms and Abbreviations

A&A	Assessment and Authorization
AIGA	Assistant Inspector General for Audit
ATO	Authority to Operate
BIA	Business Impact Assessment
CDO	Chief Data Officer
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CIO	Chief Information Officer
CSO	Cloud Service Offering
CSP	Cloud Service Provider
CUI	Controlled Unclassified Information
DOC	Department of Commerce
DOD	Department of Defense
DOE	Department of Energy
DOI	Department of the Interior
DOL	Department of Labor
DOT	Department of Transportation
EPA	Environmental Protection Agency
EXIM	Export-Import Bank
FAEC	Federal Audit Executive Council
FDIC	Federal Deposit Insurance Corporation
FedRAMP	Federal Risk and Authorization Management Program
FHFA	Federal Housing Finance Agency
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act of 2014
FRB	Board of Governors of the Federal Reserve System
GAO	Government Accountability Office
HHS	Department of Health and Human Services

IaaS	Infrastructure as a Service
IAM	Identity and Access Management
IRS	Internal Revenue Service
MFA	Multi-Factor Authentication
NASA	National Aeronautics and Space Administration
NGA	National Geospatial-Intelligence Agency
NIH	National Institutes of Health
NIST	National Institute for Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
PaaS	Platform as a Service
PII	Personally Identifiable Information
PIV	Personal Identity Verification
POA&M	Plan of Action and Milestones
SaaS	Software as a Service
SEC	U.S. Securities and Exchange Commission
SP	Special Publication
SSP	System Security Plan
TIGTA	Treasury Inspector General for the Tax Administration
USPS	United States Postal Service
VA	Department of Veterans Affairs
ZTA	Zero Trust Architecture

Acknowledgments

This report was developed under the guidance of the FAEC Cross-cutting Issues Subcommittee chaired by leadership from EXIM OIG and EPA OIG. Special thanks to the FAEC Cross-cutting Issues Subcommittee working group members who contributed their time and expertise to this effort from the following OIGs:

USPS OIG
DOI OIG
USPS OIG
FDIC OIG
DOI OIG
NGA OIG