OFFICE OF INSPECTOR GENERAL
U.S. Agency for International Development

MEMORANDUM

DATE: September 16, 2024

TO: Jason K. Gray
Chief Information Officer
USAID/Bureau for Management/Office of the Chief Information Officer

Zecharia S. Kahn
IT Operations Division Chief
USAID/Bureau for Management/Office of the Chief Information Officer

Sheila D. Wright
Deputy Chief Human Capital Officer
USAID/Office of Human Capital and Talent Management

FROM: Paul K. Martin
Inspector General

SUBJECT: Cloud Computing: USAID Needs to Improve Controls to Better Protect Agency Data (Report Number A-000-24-004-P)

USAID has increased its reliance on cloud computing services in recent years with the migration of many of its information technology (IT) operations to the cloud. According to Agency officials, USAID spent $47.6 million on cloud computing services in fiscal year 2022.

Cloud computing provides Federal agencies with "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."[1] At the same time, placing data in the cloud involves substantial risk; therefore, Federal agencies must take additional steps to protect the confidentiality, integrity, and availability of their cloud-based information. Cybersecurity compromises could result in higher costs, litigation, loss of public trust, and reputational harm.

Given these challenges, we initiated this audit to assess the extent to which USAID (1) followed selected requirements and guidelines for procuring and monitoring selected cloud computing services and (2) implemented and monitored selected security controls over selected cloud computing systems in accordance with Federal requirements.

This memorandum summarizes the results of our audit. We found that USAID did not consistently follow three of five requirements for procuring and monitoring the cloud

[1] National Institute of Standards and Technology (NIST) Special Publication (SP) 800-145, *The NIST Definition of Cloud Computing*, September 2011.

computing services we reviewed or implement and document monitoring of certain security controls. Consequently, we are making 13 recommendations to help improve the Agency's efforts to procure and secure its cloud services and systems.

After we informed USAID officials of our preliminary findings, the Agency made updates in two areas: the Agency revised access control procedures for a system's new user accounts and signed the system security plan for another system. As such, we did not make recommendations to address the related findings.

USAID agreed with all 13 recommendations. After reviewing information the Agency provided in response to the draft memorandum, we consider five recommendations closed (Recommendations 4, 5, 10, 11, and 12), seven resolved but open pending completion of planned activities (Recommendations 1, 2, 3, 6, 7, 8, and 13), and one open and unresolved (Recommendation 9).

For the eight open recommendations, please provide evidence of final action to the Audit Performance and Compliance Division.

We conducted our work at the Office of the Chief Information Officer (OCIO) and the Office of Human Capital and Talent Management (HCTM) in Washington, DC. Our audit scope covered January 1, 2020, to March 31, 2022. To answer our audit objectives, we: (1) reviewed Federal government and USAID requirements, standards, and policies applicable to cloud procurements, security controls, and monitoring; and (2) conducted interviews with Agency officials on implementation of these requirements, standards, and policies. For the first objective, we judgmentally selected a sample of 3 of 27 contracts for cloud services based on highest dollar value. For the selected contracts, we reviewed five high-risk issues that were identified in a prior audit or that we assessed as high risk based on our knowledge of procurements: (1) cost-benefit and alternative analyses, (2) acquisition plans, (3) service level agreements (SLAs), (4) contractor performance evaluations, and (5) cloud clauses. For the second objective, we judgmentally selected 2 systems from a population of 53. We selected one system because it appeared in two of our selected contracts and the other because it had the highest cost in the Agency's cloud systems inventory compared to the three contracts reviewed for the first objective. For each system, we reviewed and tested the implementation of 2 of 20 security control areas based on high-risk issues identified in past audits—(1) account management and (2) plan of action and milestones (POA&Ms) as part of security assessment, authorization, and monitoring (SAAM)—to determine whether those controls were designed and operating effectively. If not designed and properly implemented, these two high-risk controls can result in system compromise and data loss. Finally, we compared the system security plans and security assessment reports to determine whether the stated implementation status of selected controls was consistent between the two documents. We conducted our work in accordance with generally accepted government auditing standards. For full details on our scope and methodology, see Appendix A.

Background

USAID relies on third-party entities called Cloud Service Providers (CSPs) to provide platforms, applications, storage, and infrastructure support for its cloud computing services.

USAID may procure cloud services directly from CSPs or contractors may procure services on the Agency's behalf. Due to the reliance on external entities for this work, implementing effective controls is critical for protecting the confidentiality, integrity, and availability of Agency information.

The Office of Management and Budget (OMB), National Institute of Standards and Technology (NIST), and Federal Acquisition Regulation (FAR) establish government-wide requirements and standards for cloud computing. USAID's policy is outlined in the Automated Directives System (ADS) 509, "Management and Oversight of Agency Information Technology Resources," and ADS 545, "Information Systems Security," as well as the Acquisition & Assistance Policy Directive (AAPD)16-02.

Requirements and standards for procuring cloud computing services include the following:

- Performing annual evaluations of cloud computing service contractors to determine whether they have met contract terms and can continue meeting requirements.
- Including cloud-related clauses in contracts to establish expectations and hold CSPs accountable for protecting Agency information.
- Conducting cost-benefit and alternative analyses to decide whether cloud services are cost effective and align with Agency needs.
- Obtaining the Chief Information Officer's (CIO) approval of acquisition plans for awareness of services that may need to be secured.
- Using service level agreements (SLAs) to define expectations of the level of services to be performed in the contract and monitoring CSPs compliance with the SLAs.

Requirements for securing cloud computing systems include the following:

- Account management processes for approving access and authorizing roles and privileges, to prevent unauthorized access and system compromise.
- Plans of action and milestones (POA&Ms), which are part of security assessment, authorization, and monitoring (SAAM) of how security weaknesses are tracked and remediated within established timeframes.
- System security plans (SSPs) provide details about security controls in place or planned to protect an information system, and its data and must be updated when changes or issues arise.

USAID Did Not Consistently Follow Selected Requirements for Procuring and Monitoring the Sampled Cloud Computing Services

Federal requirements and USAID policies require the Agency to implement controls when procuring cloud computing services. However, we found that USAID did not consistently implement three of the five controls in the contracts we reviewed. Specifically, OCIO did not consistently conduct cost-benefit and alternative analyses, approve acquisition plans, or

implement and monitor SLA requirements. As required, OCIO officials regularly performed annual evaluations to assess whether contractor performance met the terms of the three contracts we selected for review.[2] They also included the high-risk, cloud-related clauses in the selected contracts, as required, to help protect USAID data and information.[3]

OCIO Officials Did Not Conduct Cost-Benefit and Alternative Analyses for One of Three Selected Cloud Contracts

OCIO officials provided us with cost-benefit and alternative analyses for two of the selected cloud contracts but not for the third. ADS 509.3.4.1 states:

> … when planning an IT acquisition that is not pre-approved by the CIO under the IT purchase guidance, the responsible office must … develop a comprehensive cost-benefit analysis of all procurement requirements based upon market research, which includes an analysis of alternatives (including existing Agency IT resources and solutions).

Based on our review, OCIO officials did not follow the ADS. They stated that they were not required to prepare a cost-benefit analysis because a contractor had procured the cloud system on USAID's behalf. However, Agency policy does not recognize such an exception. During this review, OCIO officials refused to provide us contract information, including "a description and an estimate of the total cost of the IT equipment, software or services." OCIO officials asserted that the information was proprietary. However, the officials should have shared it with OIG.

Further, USAID lacks specific guidance to assist staff in implementing Agency policy when considering cloud contracts. For example, ADS 509 does not provide a checklist of actions to take when conducting analyses, including a supervisory review, or address preparing and maintaining supporting documentation for cloud acquisitions. OCIO officials said that the cloud contracts were not treated differently than other IT acquisitions. As such, they said no separate guidance was needed. Nonetheless, OCIO did conduct cost-benefit and alternative analyses for two of the three selected contracts, which suggests an inconsistent application of the policy. ADS 577, "Information Technology Capital Planning and Investment Control," required all project forms and supporting documents to be maintained and submitted to the CIO.[4] However, the Agency subsequently replaced ADS 577 with ADS 509, which does not address preparing and maintaining supporting documentation for cloud acquisitions.

Without clear guidance on the need to conduct cost-benefit and alternative analyses for cloud service contracts, it is unclear whether staff are conducting these analyses to reduce procurement risks. In addition, the lack of written guidance increases the risk that cloud services procured might not be cost effective or aligned with Agency needs.

---

[2] FAR Subpart 42.15 requires an annual performance evaluation for all contracts that meet a dollar threshold.

[3] ADS 545, AAPD 16-02, and CIO and Chief Acquisition Officers Councils' *Creating Effective Cloud Computing Contracts for the Federal Government: Best Practices for Acquiring IT as a Service*. The ADS and AAPD contain USAID-specific requirements and clauses for cloud contracts.

[4] USAID developed ADS 577 in response to the recommendations in our prior report, *Audit of USAID's Progress in Adopting Cloud Computing Technologies* (A-000-15-006-P), March 12, 2015.

The Agency CIO Did Not Approve Cloud Acquisition Plans for Two of the Three Selected Contracts

The CIO approved the acquisition plan for one of the selected contracts but did not provide approval before the other two contracts were awarded. Although other OCIO officials approved these two plans, the CIO did not do so despite Federal and Agency requirements. OMB Circular A-130 states that "the CIO approves the IT components of any plans, through a process defined by the agency head."[5] Further, ADS 509.3.4.2 states that the "CIO must review and approve all acquisitions or interagency agreements that include IT at the strategy, plan, or requirement level." Moreover, that policy does not make provisions for the CIO to delegate the approval authority.

OCIO officials said that the CIO did not need to approve acquisitions because the CIO was familiar with them and had approved the related budgets, although they did not provide us with documented evidence. The officials explained that it would be too much for the CIO to approve every IT procurement and that ADS 509 did not apply to OCIO. We disagree. ADS 509.3.4.2 does not contain exceptions to the required CIO's review and approval nor does it permit delegation of this authority. Finally, OCIO did not have a written procedure for documenting the CIO's review and approval of the Agency's cloud acquisition plans. As a result, the CIO may not be aware of cloud services procured for Agency use or provide adequate oversight to ensure those services are secure.

OCIO Officials Did Not Consistently Implement or Monitor SLA Requirements for Two of Three Selected Contracts

OCIO officials did not consistently include all SLA requirements or monitor SLAs for two of the three contracts we reviewed. OMB's Cloud Smart Strategy defines SLAs as key controls for contractually defining the level of performance a customer can expect from a service provider, how performance will be measured, and what enforcement mechanisms will be used to ensure the specified levels are achieved. According to NIST Special Publication (SP) 800-144, a service agreement outlines the terms and conditions governing the use of CSP services. The SLAs for all three contracts included the minimum time for services to be operational and available and made provisions for scheduled outages in accordance with Federal guidelines and requirements.[6]

However, only the SLAs for one of the contracts included provisions for service agreement changes. NIST policy indicates that provisions should be made for changes to the service agreement to allow Agency officials to change a contract with unfavorable terms.[7] USAID did not address service agreement changes in its cloud computing SLAs or contracts—in part because OCIO officials did not have a process for determining whether SLAs met Agency

[5] OMB, Circular A-130, "Managing Information as a Strategic Resource," Section 5(3)(d), July 2016.
[6] The CIO and Chief Acquisition Officers Councils' *Creating Effective Cloud Computing Contracts for the Federal Government: Best Practices for Acquiring IT as a Service*, February 2012.
[7] NIST SP 800-146 states that "an organization should understand customer responsibilities, and those of the service provider, before using a cloud service, and that a provider may change the terms of service with a specified level of advance notice which may affect both price and quality of service. [A plan] to migrate workloads to an alternate provider should be available if a change in service terms is unacceptable."

needs. Specifically, USAID guidance did not identify the key components that should be detailed in SLAs, including provisions to build in flexibility for making changes if necessary. OCIO officials stated that they did not incorporate such changes in SLAs because they planned to renegotiate terms with the contractor through modifications if issues arose. However, due to the omission, OCIO has limited its ability to change a contract with unfavorable terms. OCIO also may not be able to easily or quickly switch service providers or migrate services in-house should a change in service terms be unacceptable, as NIST SP 800-146 cautions. Such a situation could interrupt or delay services the Agency needs to conduct its work.

In addition, OCIO officials did not provide evidence that they monitored CSP compliance with the SLAs for two of the contracts in accordance with the cloud computing guidance issued by the CIO Council and Chief Acquisition Officers Council.[8] Additionally, the Agency's AAPD 16-02 indicates that "at USAID's request, the contractor must submit reports or provide a dashboard where USAID can continuously verify that service levels are being met." Yet OCIO did not have a written policy on monitoring and documenting CSP compliance. Although OCIO officials said the CSPs had SLAs online, they could not provide evidence that they requested and reviewed reports or dashboards from the CSPs and used that information to monitor performance. OCIO officials stated that they were conducting enterprise-wide monitoring rather than monitoring individual SLAs. As a result, USAID may be unable to determine when CSPs have not met specific service levels.

Because USAID does not include all required information in SLAs or consistently monitor CSP compliance, contracted services may fall short of requirements, which may impact the Agency's ability to meet its mission.

USAID Did Not Consistently Implement and Document Monitoring of Selected Security Controls

NIST security standards for Federal information systems include controls to prevent unauthorized user access and to update plan of action and milestones (POA&M) with remediation actions taken and system security plans (SSPs) with security assessment report (SAR) results. We found that USAID system owners for two systems we reviewed did not consistently approve access or authorize roles and privileges as part of account management, update POA&Ms, or document their monitoring of the remediation of weaknesses as part of security assessment, authorization, and monitoring (SAAM). In addition, we found that Agency officials did not update the SSPs for these systems so they would be aware of weaknesses in security controls.

System Owners Did Not Consistently Approve New User Access or Authorize Roles and Privileges for Selected Systems

Account management is key to controlling system access. However, system owners[9] in HCTM

[8] Chief Information Officer Council and Chief Acquisition Officers Council, *Creating Effective Cloud Computing Contracts for the Federal Government: Best Practices for Acquiring IT as a Service,* February 2012.
[9] NIST SP 800-53 Rev. 5, *Security and Privacy Controls for Information Systems and Organizations*, defines a system owner as an "official responsible for the overall … operation, and maintenance of a system."

and OCIO's IT Operations Division did not consistently approve access or authorize roles and privileges in accordance with NIST guidance.[10] Specifically, the system owners did not approve roles and privileges for new users before granting them access to the two systems we reviewed or maintain related documentation in accordance with ADS 545.3.2.2.

We judgmentally selected 5 of 36 new users for one of the selected systems and found that system owners did not approve them before granting them access to the system. HCTM officials stated that the five users may have had a profile in the system, but they did not have access to it because they were not assigned to a group such as "users" or "system administrators." Nonetheless, documentation showed that the five users had logged into the system within 90 days of the account creation date.

For the second system, we judgmentally selected 7 of 73 new users and officials in the IT Operations Division did not provide evidence to show that these new users were approved before they received system access. The officials explained that four of the seven users had been part of the original user group when the system was set up, so they did not follow requirements for granting access. However, they did not explain why the other three users had access without prior approval.

USAID officials also did not consistently authorize account roles and privileges for the two selected systems in accordance with NIST requirements. The HCTM system owner did not authorize roles for all five selected users and authorized privileges for four of the five. The IT Operations Division's system owner did not authorize roles or privileges for any of the seven selected users.

Security and Privacy Controls for Information Systems and Organizations

NIST asserts organizations should:

- Specify (1) authorized users of the system, (2) group and role membership, and (3) access authorizations (i.e., privileges) and organizational defined attributes for each account.
- Require approvals by organizational defined personnel for requests to create accounts.
- Authorize access to the system based on (1) a valid access authorization, (2) intended system usage, (3) assignment; organization-defined attributes (as required).

NIST Special Publication (SP) 800-53 Revision 5

At the end of our audit fieldwork, OCIO officials provided us a template that they said personnel used for continuous monitoring to document system weaknesses, such as unapproved access and designation of roles and privileges. However, the template indicated it was for non-cloud systems and referred to guidance for non-cloud systems.

Also, OCIO did not take action against a system owner for not following the template. We found that while the HCTM system owner followed the template, the system owner in the IT Operations Division did not for more than a year. Further, we found that OCIO did not follow an existing procedure that would ultimately remove the system's authority to operate after 6 months of noncompliance. An OCIO official informed us, and OIG agrees, that such actions

[10] Privileges allow a user to perform certain functions, such as editing, deleting, and adding information. A role, such as system administrator, is a collection of privileges that enable a user to perform a function within a system. See also: NIST SP 800-53 Rev. 5, *Security and Privacy Controls for Information Systems and Organizations*, AC-2, "Account Management."

would disrupt a service critical for Agency operations. However, the procedure did not identify other ways to hold system owners accountable for noncompliance, such as a negative performance evaluation or disciplinary action.

Providing unapproved and unauthorized users access puts the Agency at an increased risk of system compromise. Moreover, a serious breach could lead to data loss.

System Owners Did Not Update Plans of Action and Milestones or Monitor CSP Remediation of Weaknesses

System owners did not update POA&Ms with important information—such as planned remediation actions to fix weaknesses—or document how they monitored CSPs' remediation of weaknesses for the selected systems. ADS 545.3.5.4 requires POA&Ms, which are an important control for tracking planned actions to remediate identified weaknesses. However, HCTM and the IT Operations Division did not update POA&Ms for identified weaknesses on a quarterly basis, as required during testing, and failed to include planned remediation actions.[11]

Plan of Actions and Milestone

"When information system weaknesses or deficiencies are noted during assessments, audits, or other security related activities, [system owners] must develop Plans of Action and Milestones (POA&M) to document the planned remedial actions and update the POA&M at least quarterly based on security monitoring activities."

ADS 545.3.5.4

In addition, the system owner in the IT Operations Division did not document the monitoring of the CSP's remediation activities for one of the selected systems. As discussed above, OCIO had a process to escalate system owners' noncompliance that would ultimately deny a system's authority to operate after 6 months. However, the responsible officials did not follow this process to avoid disrupting services critical for Agency operations. Moreover, other ways to hold system owners accountable for noncompliance, such as a negative performance evaluation or disciplinary action, were not included in the escalation procedure.

According to NIST, agencies are to "update existing plan[s] of action and milestones … based on the findings from control assessments, independent audits or reviews, and continuous monitoring activities."[12] ADS 545 requires POA&Ms to follow "either NIST or USAID-defined continuous monitoring activities as agreed to in a continuous monitoring plan to monitor security control compliance by external service providers on an ongoing basis." However, ADS 545 did not require system owners to document their monitoring activities, such as updating POA&Ms. By not documenting and monitoring remediation activities, USAID has limited its ability to adequately track progress and manage risk.

Responsible USAID Officials Did Not Fully Update Selected System Security Plans

System security plans (SSPs) provide details about the security controls in place or planned to

[11] USAID ADS 545.3.5.4, "Plan of Actions and Milestones," March 2021 version was applicable during testing, but the Agency revised it in December 2022.
[12] NIST SP 800-53 Rev. 5, CA-5, "Plan of Action and Milestones."

protect an information system, and its data and must be updated when the system or environment changes or problems arise. The SSP plays an important role because it describes the security requirements for an information system and the plan and status of meeting those requirements. In turn, a security assessment report (SAR) documents an assessor's findings and recommendations for correcting security control weaknesses. Our review found that HCTM and IT Operations Division officials did not fully update the SSPs for the two selected systems to reflect the implementation status of selected security controls as reported in the SAR.

NIST SP 800-53 requires system owners to develop SSPs and update them with the control assessment results documented in the SAR. NIST identifies 23 access controls and 8 SAAM controls important for assessing and monitoring the effectiveness of system controls.

Our comparison of the SARs and SSPs for the two selected systems revealed that system owners did not update the SSPs to reflect what was reported in the SARs. For one of the selected systems, HCTM officials did not update two access controls and two SAAM controls in the SSP. For the other system, IT Operations Division officials did not update three access controls in the SSP to reflect the SAR for more than 2 years.

System Security Plan

According to NIST, system owners must:

- Develop security plans for the system that … [d]escribe the controls in place or planned for meeting the security … requirements;
- Update the plans to address changes to the system and environment of operation or problems identified during plan implementation or control assessments; and
- Develop security plans for the system that … [a]re reviewed and approved by the authorizing official or designated representative prior to plan implementation.

NIST SP 800-53, Revision 5

USAID's risk management procedure states that after an issue is identified, the system owner and information system security officer[13] have one day to make corrections to the SSP.[14] After one day, the system owner should create a POA&M if the updates to the SSP are not completed. However, HCTM and IT Operations Division officials did not update the SSPs or create POA&Ms for the two systems we reviewed. The lack of an SSP that is continuously updated to reflect the current status of the security controls could leave the Agency unaware of weaknesses that might cause a security breach.

Conclusion

Cloud services are an integral part of USAID's operations. To mitigate associated risks, the Agency has developed and implemented controls to protect the confidentiality, integrity, and availability of information stored in the cloud. However, by adding controls and consistently implementing existing controls, USAID can more effectively procure, monitor, and use cloud computing services. Strengthening these controls will put the Agency in a better position to use taxpayer dollars more efficiently while protecting system data.

[13] The NIST glossary defines an information system security officer as an "individual with assigned responsibility for maintaining the appropriate operational security posture for a system or program."
[14] USAID, *Information Technology (IT) Systems Accreditation Risk Management Framework (RMF) Handbook*, v2.0, July 17, 2023.

Recommendations

We recommend that the USAID Chief Information Officer take the following actions:

1. Develop and implement written guidance for performing and documenting cost-benefit and alternative analyses for cloud acquisitions before procuring cloud services.
2. Develop and implement a written procedure to document the Chief Information Officer's review and approval of all cloud service acquisition plans.
3. Develop and implement a written process for defining and reviewing service level agreements to determine whether they meet Agency needs.
4. Develop and implement a written policy for monitoring and documenting cloud services providers' compliance with service level agreements.
5. Revise the standard reporting template for continuous monitoring to clarify whether it applies to cloud systems.
6. Develop additional procedures to hold system owners accountable for noncompliance with continuous monitoring reporting requirements. This may include actions other than denying a system authority to operate, such as a negative performance evaluation or disciplinary action.
7. Develop additional procedures to hold system owners accountable for noncompliance with plan of action and milestones requirements. This may include actions other than denying a system authority to operate, such as a negative performance evaluation or disciplinary action.
8. Revise Agency procedures to address how system owners should document their monitoring of cloud service providers' remediation activities.
9. Work with the Deputy Chief Human Capital Officer and IT Operations Division Chief to update the system security plan, as required. This may include updating the system security plan with the results of a security assessment or create a plan of action and milestones.

We recommend that USAID's Deputy Chief Human Capital Officer:

10. Update the system's continuous monitoring report to identify weaknesses with access, roles, and privileges, as required.
11. Complete plan of action and milestones, as required. This may include documenting the "planned remediation actions" in the reports.

We recommend that USAID's IT Operations Division Chief:

12. Update the systems' continuous monitoring report to identify weaknesses with access, roles, and privileges, as required.
13. Complete plan of action and milestones, as required. This may include documenting the "planned remediation actions" in the reports.

OIG RESPONSE TO AGENCY COMMENTS

We provided our draft report to USAID on July 15, 2024. On August 19, 2024, we received the Agency's response, which is included in Appendix B of this report excluding the supporting documentation.

The report included 13 recommendations, and we acknowledge management decisions on all of them. We consider five of them closed (Recommendations 4, 5, 10, 11, and 12), seven resolved but open pending completion of planned activities (Recommendations 1, 2, 3, 6, 7, 8, and 13), and one unresolved (Recommendation 9) for the reason below.

USAID did not provide sufficient documentation of its final action for Recommendation 9. For one system, Agency officials provided an updated system security plan that included the results of its security assessment or created plans of action and milestones. However, officials did not provide an updated system security plan for the other system. As a result, we cannot close the recommendation as requested.

Appendix A. Scope and Methodology

We conducted our work from July 8, 2021, through July 15, 2024, in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Our audit objectives were to assess the extent to which USAID (1) followed selected requirements and guidelines for procuring and monitoring selected cloud computing services and (2) implemented and monitored selected security controls over selected cloud computing systems in accordance with Federal requirements.

In planning and performing the audit, we gained an understanding of and assessed internal controls that were significant to the audit objectives. Specifically, we designed and conducted procedures related to all five components of internal control as defined by the U.S. Government Accountability Office (GAO): Control Environment, Risk Assessment, Control Activities, Information and Communication, and Monitoring.[15]

The audit covered January 1, 2020, to March 31, 2022. We also reviewed relevant changes USAID made to ADS guidance in December 2022. Audit work covered USAID's OCIO, including the IT Operations Division and the Office of Human Capital and Talent Management HCTM at the Agency's headquarters in Washington, DC. We covered OCIO because that office is responsible for cloud services and implementing security controls within the scope of this audit. We also covered the IT Operations Division and HCTM because they owned the selected systems. We performed our work in Washington, DC.

In answering the objectives, we reviewed applicable laws, Federal and USAID acquisition policies, NIST publications, OMB guidance, and USAID ADS chapters. We interviewed Agency officials and reviewed supporting documentation.

To answer the first objective, we used computer-processed data. Specifically, we used data in USAID's inventory listing to judgmentally select three active cloud contracts active within the last year as of March 31, 2022. To determine the reliability of data in the inventory listing, which included cloud systems, contracts, and their values, we interviewed Agency officials to gain an understanding of the inventory itself. We also traced the system inventory as of June 30, 2021, to the overall system inventory we used for our fiscal year 2021 audit pursuant to the Federal Information Security Modernization Act of 2014. In addition, for a sample of cloud contracts, we compared the values in the contracts themselves to the Agency's financial reporting database and its acquisition and assistance system. We determined that the data was sufficiently reliable for the purposes of our audit.

To determine whether USAID followed selected requirements and guidelines for procuring and monitoring, we reviewed five high-risk issues that were either identified in a prior audit or that we assessed as high risk based on our knowledge of procurements: (1) cost-benefit and alternative analyses, (2) acquisition plans, (3) service level agreements (SLAs), (4) contractor

[15] GAO, *Standards for Internal Control in the Federal Government* (GAO-14-704G), September 10, 2014.

performance evaluations, and (5) cloud clauses. We also reviewed Agency acquisition policies and procedures as well as selected requirements and guidelines for Federal cloud acquisitions based on those identified five high-risk areas as prescribed by FAR 7.102 and ADS 545.

To make a judgmental sample selection, we reviewed the Agency's inventory listing of contracts for cloud systems, which identified 27 contracts with cloud services. From this list, we judgmentally selected the three highest priced contracts with cloud services and reviewed selected documentation, such as business cases, to determine justification for cloud service acquisition as prescribed by NIST SP 800-35 and ADS 509. We did not project the results of our testing to the population of cloud contracts but determined that our selection method was appropriate and generated valid, reliable evidence for the objective.

For the three selected contracts, we:

- Reviewed documentation to determine whether USAID officials conducted cost-benefit analyses as prescribed by FAR 39.102, OMB's *Capital Programming Guide*, and ADS 509.
- Reviewed analyses of alternatives to determine whether the Agency chose the best course of action in terms of risk and costs as prescribed by FAR 39.102 and ADS 509.
- Determined whether the CIO reviewed and approved plans and acquisitions for the contracts before acquiring the cloud services as prescribed by OMB A-130 and ADS 509.
- Reviewed the contracts to determine whether they contained the high-risk cloud-related clauses as prescribed by ADS 545, AAPD 16-02, and the CIO and Chief Acquisition Officers Councils' *Creating Effective Cloud Computing Contracts for the Federal Government: Best Practices for Acquiring IT as a Service*. We selected the cloud-related clauses based on what we believe are high-risk areas, such as security requirements, data ownership, data location, limitations on access, and disclosure of Agency information.
- Reviewed SLAs to determine whether the Agency defined service level expectations, the contract language included service agreement changes and planned for outages, and the Agency monitored service levels as prescribed by *Creating Effective Cloud Computing Contracts for the Federal Government: Best Practices for Acquiring IT as a Service*, NIST SP 800-146, and NIST SP 800-35.

For the second audit objective, we reviewed data in the POA&M and system user listings. To determine the reliability of the data in these listings, we interviewed Agency officials to gain an understanding of the data elements and the queries used to generate them. We also observed Agency officials as they ran those queries. We then compared the queries parameters to the listings themselves. We determined that the data was sufficiently reliable for the purposes of our audit.

In addition, we judgmentally selected 2 systems from a population of 40. We selected one system because it appeared in two of our selected contracts and the other because, of the three contracts we reviewed for the first objective, it had the highest cost in the Agency's cloud systems inventory. For our assessment of account management controls, we determined our sample sizes based on the frequency of the control being tested for each system. We selected a minimum sample size of 10 percent of the medium populations (i.e., 50 to 250 users of a population). For small populations (i.e., fewer than 50 users of a population), we selected a minimum sample size of 5 users and 100 percent where the population was less than 5 users.

We used a random number generator to select the samples. Using this methodology, we selected 5 of 36 new users for one system and 7 of 73 users for the other system. Due to the nature of our sampling, we were unable to project the results of our samples to the entire population of cloud systems or controls. However, we determined that the samples were appropriate for our audit objective and produced valid, reliable evidence.

In addition:

- For the two judgmentally selected systems discussed above, we reviewed the implementation of specific sections of 2 of 20 security control areas based on high-risk issues identified in past audits—account management and POA&Ms as part of SAAM—to determine whether security controls were designed and operating effectively, as prescribed by NIST SP 800-53 Rev. 5 and ADS 545. We selected these two high-risk areas because weaknesses can result in system compromise and data loss.
- We compared the SSPs and SARs for the two selected systems to determine whether the stated implementation status of selected controls was consistent, as prescribed by NIST SP 800-53 Rev. 5 and ADS 545.

Appendix B. Agency Management Comments

MEMORANDUM

TO: Deputy Assistant Inspector General for Audit, Gabriele A. Tonsil

FROM: USAID/Bureau for Management/Chief Information Officer, Jason K. Gray /s/

DATE: August 20, 2024

SUBJECT: Management Comments to Respond to the Draft Audit Report Produced by the Office of Inspector General (OIG) titled, *Cloud Computing: USAID Needs to Improve Controls to Better Protect Agency Data* (Task No. AA100720)

The U.S. Agency for International Development (USAID) would like to thank the Office of Inspector General (OIG) for the opportunity to provide comments on the subject draft report. The Agency agrees with the recommendations, herein provides evidence of compliance with them, plans for implementing them, and reports on significant progress already made.

The OIG's evaluations provide a valuable opportunity to assess and improve upon USAID's policies, procedures, and programs. Thank you for the opportunity to respond to your final report, and for the courtesy shown by your staff while conducting this engagement.

COMMENTS BY THE U.S. AGENCY FOR INTERNATIONAL DEVELOPMENT (USAID) ON THE REPORT RELEASED BY THE USAID OFFICE OF THE INSPECTOR GENERAL (OIG) TITLED, *Cloud Computing: USAID Needs to Improve Controls to Better Protect Agency Data* (Task No. AA100720)

Please find below the management comments from the U.S. Agency for International Development (USAID) on the draft report produced by the Office of the USAID Inspector General (OIG), which contains 13 recommendations for USAID recommendations:

Recommendation 1: We recommend that the USAID Chief Information Officer: Develop and implement written guidance for performing and documenting cost-benefit and alternative analyses for cloud acquisitions before procuring cloud services.

- **Management Comments:** M/CIO agrees with the recommendation. M/CIO will formally document and implement a revised process for performing and documenting cost-benefit and alternative analyses before procuring cloud services.

- **Target Completion Date:** 09/15/2025

Recommendation 2: We recommend that the USAID Chief Information Officer: Develop and implement a written procedure to document the Chief Information Officer's review and approval of all cloud service acquisition plans.

- **Management Comments:** M/CIO agrees with the recommendation. M/CIO will develop and implement a written process to document the Chief Information Officer's review and approval of all cloud service acquisition plans.

- **Target Completion Date:** 09/15/2025

Recommendation 3: We recommend that the USAID Chief Information Officer: Develop and implement a written process for defining and reviewing service level agreements to determine whether they meet Agency needs.

- **Management Comments:** M/CIO agrees with the recommendation. M/CIO will develop and implement a written process for defining and reviewing service level agreements to determine whether they meet Agency needs.

- **Target Completion Date:** 09/15/2025

Recommendation 4: We recommend that the USAID Chief Information Officer: Develop and implement a written policy for monitoring and documenting cloud services providers' compliance with service level agreements.

- **Management Comments:** M/CIO agrees with the recommendation to develop and implement a written policy for monitoring and documenting cloud services providers' compliance with service level agreements. M/CIO revised ADS 302mah, Information Security Requirements for Acquisition of Unclassified Information Technology to provide guidance on service level agreements for cloud computing in awards. The policy was issued on May 31, 2024. M/CIO requests this recommendation be closed upon issuance.

- **Target Completion Date:** Closure upon issuance of the final report.

Recommendation 5: We recommend that the USAID Chief Information Officer: Revise the standard reporting template for continuous monitoring to clarify whether it applies to cloud systems.

- **Management Comments:** M/CIO agrees with the recommendation. While the reporting template for continuous monitoring has always applied to cloud systems, we have revised the title of the document to ensure clarity.

- **Target Completion Date:** Closure upon issuance of the final report.

Recommendation 6: We recommend that the USAID Chief Information Officer: Develop additional procedures to hold system owners accountable for noncompliance with continuous monitoring reporting requirements. This may include actions other than denying a system authority to operate, such as a negative performance evaluation or disciplinary action.

- **Management Comments:** M/CIO agrees with the recommendation. We plan to update the USAID Letter of Designation As System Owner (SO) Template which is a tool to hold system owners accountable. It will include language that will notify the SO's supervisor if they are non-compliant and recommend whether the supervisor take action. If the supervisor fails to take action we will then report this issue to Employee and Labor Relations.

- **Target Completion Date:** 03/15/2025

Recommendation 7: We recommend that the USAID Chief Information Officer: Develop additional procedures to hold system owners accountable for noncompliance with plan of action and milestones requirements. This may include actions other than denying a system authority to operate, such as a negative performance evaluation or disciplinary action.

- **Management Comments:** M/CIO agrees with the recommendation. We plan to update the USAID Letter of Designation As System Owner (SO) Template which is a tool to hold system owners accountable. It will include language that will notify the SO's supervisor if they are non-compliant and recommend whether the supervisor take action. If the supervisor fails to take action, we will then report this issue to Employee and Labor Relations.

- **Target Completion Date:** 03/15/2025

Recommendation 8: We recommend that the USAID Chief Information Officer: Revise Agency procedures to address how system owners should document their monitoring of cloud service providers' remediation activities.

- **Management Comments:** M/CIO agrees with the recommendation. M/CIO will revise to address how system owners should document their monitoring of cloud service providers' remediation activities.

Target Completion Date: 09/15/2025

Recommendation 9: We recommend that the USAID Chief Information Officer: Work with the Deputy Chief Human Capital Officer and IT Operations Division Chief to update the system security plan, as required. This may include updating the system security plan with the results of a security assessment or create a plan of action and milestones.

- **Management Comments:** M/CIO agrees with the recommendation. M/CIO has already worked with the Deputy Chief Human Capital Officer to update the system security plan, as required. M/CIO has already worked with the IT Operations Division Chief and updated the system security plan as required. M/CIO requests this recommendation be closed upon issuance.

- **Target Completion Date:** Closure upon issuance of the final report.

Recommendation 10: We recommend that USAID's Deputy Chief Human Capital Officer: Update the system's continuous monitoring report to identify weaknesses with access, roles, and privileges, as required.

- **Management Comments:** The Office of Human Capital and Asset Management agrees with the recommendation. The system's continuous monitoring report has been updated to include review of user account request forms. The system's Account Management procedures were also updated to include NIST 800-53 Rev 5 controls and the need to have user account requests approved before account creation. HCTM requests this recommendation be closed upon issuance.

- **Target Completion Date:** Closure Upon Issuance of the final report.

Recommendation 11: We recommend that USAID's Deputy Chief Human Capital Officer: Complete plan of action and milestones, as required. This may include documenting the "planned remediation actions" in the reports.

- **Management Comments:** The Office of Human Capital and Asset Management agrees with the recommendation. The system's Plan of Actions & Milestones (POAMs) are updated monthly as part of the Continuous Monitoring activity. POAMs not closed are updated in a separate milestone detailing current status. There is currently only one open POAM for the system, requiring cross Agency coordination to resolve. HCTM requests this recommendation be closed upon issuance.

- **Target Completion Date:** Closure Upon Issuance of the final report.

Recommendation 12: We recommend that the USAID Chief Information Officer: Update the systems' continuous monitoring report to identify weaknesses with access, roles, and privileges, as required.

- **Management Comments:** M/CIO agrees with the recommendation. M/CIO has already worked with the IT Operations Division Chief and updated the systems' continuous monitoring report to identify weaknesses with access, roles, and privileges, as required. M/CIO requests this recommendation be closed upon issuance.

- **Target Completion Date:** Closure Upon Issuance of the final report.

Recommendation 13: We recommend that the USAID Chief Information Officer: Complete plan of action and milestones, as required. This may include documenting the "planned remediation actions" in the reports.

- **Management Comments:** M/CIO agrees with the recommendation. M/CIO will work with the IT Operations Division Chief and complete the system's plan of action and milestones, as required.

- **Target Completion Date:** 09/15/2025