



United States Government Accountability Office

---

Report to the Ranking Member  
Subcommittee on Cybersecurity, Information  
Technology and Government Innovation  
Committee on Oversight and Accountability  
House of Representatives

---

September 2024

# CLOUD COMPUTING

## Agencies Need to Address Key OMB Procurement Requirements

# GAO Highlights

Highlights of [GAO-24-106137](#), a report to Ranking Member of the Subcommittee on Cybersecurity, Information Technology and Government Innovation, Committee on Oversight and Accountability, House of Representatives

## Why GAO Did This Study

Cloud computing enables on-demand access to shared computing resources, providing services more quickly and at a lower cost than having agencies maintain these resources themselves. In 2010, OMB began requiring agencies to shift their IT services to cloud services when feasible. In 2019, OMB updated its Federal Cloud Computing Strategy (called Cloud Smart) and established five key cloud procurement requirements.

GAO was asked to examine agencies' efforts to implement OMB's Cloud Smart initiative. This report assesses the extent to which agencies' cloud guidance addresses OMB's five Cloud Smart procurement requirements. For each of the 24 Chief Financial Officers Act agencies, GAO analyzed relevant cloud procurement and security policies, guidance, and SLAs. GAO then assessed the results of the analysis against the five requirements. GAO also interviewed officials in the 24 agencies' Offices of the CIO.

## What GAO Recommends

GAO is making one recommendation to the CIO Council to collect and share examples of guidance on cloud SLAs and contract language. GAO is also making 46 recommendations to 18 agencies to develop or update guidance related to OMB's Cloud Smart procurement requirements. Fourteen agencies agreed with all recommendations, one agency did not explicitly agree but provided planned actions, the CIO Council and three agencies neither agreed nor disagreed, and one (Department of Education) disagreed. GAO continues to believe its recommendation to Education is warranted, as discussed in this report.

View [GAO-24-106137](#). For more information, contact Carol Harris at (202) 512-4456 or [HarrisCC@gao.gov](mailto:HarrisCC@gao.gov).

September 2024

## CLOUD COMPUTING

### Agencies Need to Address Key OMB Procurement Requirements

## What GAO Found

Agencies had mixed results in setting policies and guidance that addressed the five key procurement requirements established by the Office of Management and Budget (OMB) in its 2019 Cloud Smart Strategy. Specifically, as of July 2024, all 24 agencies had established guidance to ensure the agency Chief Information Officer (CIO) oversaw modernization and almost all had guidance in place to improve their policies and guidance related to cloud services. However, most agencies did not establish guidance related to service level agreements (SLA), which define the levels of service and performance that the agency expects its cloud providers to meet. In addition, nearly one-third of agencies did not have guidance to ensure continuous visibility in high value assets (systems that process high-value information or serve a critical function in maintaining the security of the civilian enterprise).

**Table 1: Extent to Which Federal Agencies' Guidance Has Addressed the Five Procurement-Related Cloud Computing Requirements, as of July 2024**

Requirement	Fully Addressed	Partially Addressed	Not Addressed
Ensure the agency's chief information officer oversees modernization.	24	0	0
Iteratively improve agency policies and guidance.	23	0	1
Have cloud service level agreement in place.	6	10	8
Standardize cloud contract service level agreements	9	2	13
Ensure continuous visibility in high value asset contracts. <sup>a</sup>	11	2	5

Legend: Fully addressed = The agency provided evidence that addressed the requirement. Partially addressed = The agency provided evidence that it had addressed some, but not all of the requirement. Not addressed = The agency did not provide evidence that it had addressed any of the requirement.

Source: GAO analysis of agency documentation. | GAO-24-106137

<sup>a</sup>The requirement was not applicable for six agencies because high value assets were not stored in the cloud.

Agency officials provided different reasons as to why guidance had not been developed for the requirements. For example, six agencies reported that they had used SLAs provided by the cloud service providers. One agency reported that it had included language in its blanket purchase agreement and two agencies reported they were in the process of finalizing guidance. Regarding high value asset guidance, one agency reported that it had included language in their contracts to meet the requirement but had not developed corresponding guidance. One agency reported that it had relied on standard acquisition practices and had not developed separate processes for these assets.

In addition, agency officials reported that additional guidance, including standardized SLA language and high value asset contract language, would be helpful. The CIO Council, as a forum for improving agency practices, could facilitate the collection of examples of guidance and language from agencies that have met these requirements. By sharing examples of agency guidance and contract language related to the SLA and high value asset requirements, agencies would be able to more readily address OMB's requirements.

---

# Contents

---

Letter		1
	Background	4
	Agencies Had Mixed Results in Establishing Guidance for All Key Procurement Requirements Included in OMB's Cloud Smart Strategy	11
	Conclusions	24
	Recommendations for Executive Action	24
	Agency Comments and Our Evaluation	31
Appendix I	Analysis of Federal Agencies' Guidance to Address OMB's Procurement-Related Cloud Computing Requirements	38
Appendix II	Comments from the Department of Commerce	64
Appendix III	Comments from the Department of Education	67
Appendix IV	Comments from the Department of Energy	68
Appendix V	Comments from the Department of Health and Human Services	71
Appendix VI	Comments from the Department of Homeland Security	73
Appendix VII	Comments from the Department of Housing and Urban Development	76
Appendix VIII	Comments from the Department of Veterans Affairs	82

Appendix IX	Comments from the Environmental Protection Agency	85
Appendix X	Comments from the General Services Administration	88
Appendix XI	Comments from the National Science Foundation	89
Appendix XII	Comments from the Nuclear Regulatory Commission	90
Appendix XIII	Comments from the Office of Personnel Management	94
Appendix XIV	Comments from the Small Business Administration	95
Appendix XV	Comments from the Social Security Administration	97
Appendix XVI	Comments from the U.S. Agency for International Development	98
Appendix XVII	GAO Contact and Staff Acknowledgments	100

Tables

Table 1: Key Procurement Cloud Computing Requirements in OMB's Cloud Smart Strategy	6
Table 2: Ten Key Practices for a Cloud Computing Service Level Agreement (SLA)	9
Table 3: Extent to Which Federal Agencies' Guidance Addressed the Five Office of Management and Budget Procurement-Related Cloud Computing Requirements, as of July 2024	13

---

Table 4: Coverage of Required Elements by 10 Agencies with Guidance that Partially Addressed Office of Management and Budget’s Requirements for Cloud Service Level Agreements, as of July 2024	17
Table 5: Key Procurement Cloud Computing Requirements in OMB’s <i>Federal Cloud Computing Strategy</i>	38
Table 6: Extent to Which Department of Agriculture Guidance Has Addressed the Five OMB Procurement-Related Cloud Requirements, as of July 2024	39
Table 7: Extent to Which Department of Commerce Guidance Has Addressed the Five OMB Procurement-Related Cloud Requirements, as of July 2024	40
Table 8: Extent to Which Department of Defense Guidance Has Addressed the Five OMB Procurement-Related Cloud Requirements, as of July 2024	42
Table 9: Extent to Which Department of Education Guidance Has Addressed the Five OMB Procurement-Related Cloud Requirements, as of July 2024	42
Table 10: Extent to Which Department of Energy Guidance Has Addressed the Five OMB Procurement-Related Cloud Requirements, as of July 2024	44
Table 11: Extent to Which Department of Health and Human Services (HHS) Guidance Has Addressed the Five OMB Procurement-Related Cloud Requirements, as of July 2024	45
Table 12: Extent to Which Department of Homeland Security (DHS) Guidance Has Addressed the Five OMB Procurement-Related Cloud Requirements, as of July 2024	46
Table 13: Extent to Which Department of Housing and Urban Development (HUD) Guidance Has Addressed the Five OMB Procurement-Related Cloud Requirements, as of July 2024	47
Table 14: Extent to Which Department of the Interior Guidance Has Addressed the Five OMB Procurement-Related Cloud Requirements, as of July 2024	48
Table 15: Extent to Which Department of Justice Guidance Has Addressed the Five OMB Procurement-Related Cloud Requirements, as of July 2024	49
Table 16: Extent to Which Department of Labor Guidance Has Addressed the Five OMB Procurement-Related Cloud Requirements, as of July 2024	50

---

Table 17: Extent to Which Department of State Guidance Has Addressed the Five OMB Procurement-Related Cloud Requirements, as of July 2024	51
Table 18: Extent to Which Department of Transportation Guidance Has Addressed the Five OMB Procurement-Related Cloud Requirements, as of July 2024	52
Table 19: Extent to Which Department of the Treasury Guidance Has Addressed the Five OMB Procurement-Related Cloud Requirements, as of July 2024	53
Table 20: Extent to Which Department of Veterans Affairs (VA) Guidance Has Addressed the Five OMB Procurement-Related Cloud Requirements, as of July 2024	54
Table 21: Extent to Which Environmental Protection Agency (EPA) Guidance Has Addressed the Five OMB Procurement-Related Cloud Requirements, as of July 2024	55
Table 22: Extent to Which General Services Administration (GSA) Guidance Has Addressed the Five OMB Procurement-Related Cloud Requirements, as of July 2024	56
Table 23: Extent to Which National Aeronautics and Space Administration (NASA) Guidance Has Addressed the Five OMB Procurement-Related Cloud Requirements, as of July 2024	57
Table 24: Extent to Which National Science Foundation (NSF) Guidance Has Addressed the Five OMB Procurement-Related Cloud Requirements, as of July 2024	58
Table 25: Extent to Which Nuclear Regulatory Commission (NRC) Guidance Has Addressed the Five OMB Procurement-Related Cloud Requirements, as of July 2024	59
Table 26: Extent to Which Office of Personnel Management (OPM) Guidance Has Addressed the Five OMB Procurement-Related Cloud Requirements, as of July 2024	60
Table 27: Extent to Which Small Business Administration (SBA) Guidance Has Addressed the Five OMB Procurement-Related Cloud Requirements, as of July 2024	61
Table 28: Extent to Which Social Security Administration (SSA) Guidance Has Addressed the Five OMB Procurement-Related Cloud Requirements, as of July 2024	62

---

Table 29: Extent to Which U.S. Agency for International Development (USAID) Guidance Has Addressed the Five OMB Procurement-Related Cloud Requirements, as of July 2024

---

**Abbreviations**

CIO	chief information officer
CISA	Cybersecurity and Infrastructure Security Agency
DHS	Department of Homeland Security
EPA	Environmental Protection Agency
FedRAMP	Federal Risk and Authorization Management Program
GSA	General Services Administration
GWAC	governmentwide acquisition contract
HHS	Department of Health and Human Services
HUD	Department of Housing and Urban Development
HVA	high value asset
NASA	National Aeronautics and Space Administration
NRC	Nuclear Regulatory Commission
NSF	National Science Foundation
OMB	Office of Management and Budget
OPM	Office of Personnel Management
SBA	Small Business Administration
SLA	service level agreement
SSA	Social Security Administration
USAID	U.S. Agency for International Development
VA	Department of Veterans Affairs

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



September 10, 2024

The Honorable Gerald E. Connolly  
Ranking Member  
Subcommittee on Cybersecurity, Information Technology, and  
Government Innovation  
Committee on Oversight and Accountability  
House of Representatives

Dear Mr. Connolly:

Over the past 2 decades, the federal government’s increasing demand for IT has led to a dramatic rise in operational costs to develop, implement, and maintain its computer systems and services. Furthermore, while federal agencies’ IT use provides essential services affecting the health, economy, and defense of the nation, this use has also led to a reliance on custom IT systems that can be costly to maintain. In fiscal year 2025, the proposed Federal budget describes plans to spend approximately \$139.23 billion on IT investments.<sup>1</sup>

As part of a comprehensive effort to transform IT within the federal government, in 2010, the Office of Management and Budget (OMB) began requiring agencies to shift their IT services to a cloud computing service (cloud services) option when feasible.<sup>2</sup> According to the National Institute of Standards and Technology, cloud computing is a means for enabling on-demand access to shared pools of configurable computing resources (e.g., networks, servers, storage applications, and services) that can be rapidly provisioned and released. Cloud services offer federal agencies a means to buy services more quickly and possibly at a lower cost than building, operating, and maintaining these computing resources themselves.

To accelerate agency adoption of cloud services, in June 2019, OMB published its updated *Federal Cloud Computing Strategy*, called Cloud

---

<sup>1</sup>Office of Management and Budget, *Analytical Perspectives, Budget of the U.S. Government, Fiscal Year 2025* (Washington, D.C.: Mar. 11, 2024); Department of Defense, *Department of Defense Information Technology and Cyberspace Activities Budget Overview: President’s Budget 2025 Budget Request* (March 2024).

<sup>2</sup>Office of Management and Budget, *25 Point Implementation Plan to Reform Federal Information Technology Management* (Dec. 9, 2010).



---

Smart.<sup>3</sup> As part of Cloud Smart, OMB required all federal agencies to rationalize their application portfolios—streamlining the portfolio with the goal of improving efficiency, reducing complexity and redundancy, and lowering the cost of ownership—to drive cloud adoption. In addition, OMB called for agencies to implement five key requirements within the area of procurement to help ensure successful cloud implementation.

You asked us to review agencies' efforts to address OMB's Cloud Smart initiative. Our objective was to determine the extent to which federal agencies' cloud computing guidance address the five procurement-related requirements included in OMB's *Federal Cloud Computing Strategy*.

To address this objective, we selected the 24 Chief Financial Officers Act agencies for this review because these agencies were all required to implement the five requirements under Cloud Smart. These agencies are the Department of Agriculture, Department of Commerce, Department of Defense, Department of Education, Department of Energy, Department of Health and Human Services (HHS), Department of Homeland Security (DHS), Department of Housing and Urban Development (HUD), Department of the Interior, Department of Justice, Department of Labor, Department of State, Department of Transportation, Department of the Treasury, Department of Veterans Affairs (VA), Environmental Protection Agency (EPA), General Services Administration (GSA), National Aeronautics and Space Administration (NASA), National Science Foundation (NSF), Nuclear Regulatory Commission (NRC), Office of Personnel Management (OPM), Small Business Administration (SBA), Social Security Administration (SSA), and the U.S. Agency for International Development (USAID).

We analyzed each of the 24 agencies' policies and processes related to cloud services against the five requirements we identified in OMB's Cloud Smart initiative in prior work to determine whether the agency's guidance had addressed them.<sup>4</sup> We focused on whether the 24 agencies had developed agency-wide policies and other guidance that addressed OMB's requirements because OMB Circular A-130 requires agency Chief Information Officers (CIO) to define policies and processes in sufficient

---

<sup>3</sup>Office of Management and Budget, *Federal Cloud Computing Strategy* (June 24, 2019).

<sup>4</sup>GAO, *Cloud Computing: DOD Needs to Improve Workforce Planning and Software Application Modernization*, [GAO-22-104070](#) (Washington, D.C.: June 29, 2022).

---

detail for all information resources.<sup>5</sup> This included documentation such as agencies' cloud strategies, cloud procurement and security-related guidance, contract clauses, statements of work, as well as related directives and service level agreements.

In performing our analysis, we determined the extent to which the agencies had established policies and guidance for implementing each requirement—by rating them as fully addressed, partially addressed, or not addressed.<sup>6</sup> For the requirement regarding ensuring language was included in contracts for high value assets (HVA),<sup>7</sup> we also assigned an additional rating of not applicable if the requirement did not apply to the agency as it had no high value assets stored in the cloud. Six agencies did not have HVAs stored in the cloud, and therefore, we did not assess them against this requirement.

We also corroborated our analysis by interviewing officials in the 24 agencies' Office of the CIO, Office of the Chief Acquisition Officer or Office of the Senior Procurement Executive regarding the agency's guidance and other documentation related to cloud services in the area of procurement.

We conducted this performance audit from June 2022 to September 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.

---

<sup>5</sup>Office of Management and Budget, *Managing Information as a Strategic Resource*, Circular A-130 (July 28, 2016).

<sup>6</sup>Fully addressed: The agency provided guidance that addressed the requirement; Partially addressed: The agency provided guidance that addressed some, but not all of the requirement; Not addressed: The agency did not provide guidance that addressed any of the requirement.

<sup>7</sup>A high value asset is a designation for federal information or a federal information system that processes, stores, or transmits high-value information, is considered vital to an agency fulfilling its primary mission, or serves a critical function in maintaining the security and resilience of the Federal civilian enterprise.

---

## Background

Cloud computing is a means for enabling on-demand access to shared pools of configurable computing resources (e.g., networks, servers, storage applications, and services) that can be rapidly provisioned. More specifically, purchasing IT services through a cloud service provider enables agencies to avoid paying for all the computing resources that would typically be needed to provide such services. This approach offers federal agencies a means to buy services more quickly and possibly at a lower cost than building, operating, and maintaining these computing resources themselves.

According to the National Institute of Standards and Technology, cloud computing offers federal agencies a number of benefits:

- **On-demand self-service.** Agencies can, as needed, provision computing capabilities, such as server time and network storage, from the service provider automatically and without human interaction.
- **Broad network access.** Agencies can access needed capabilities over the network through workstations, laptops, or other mobile devices.
- **Resource pooling.** Agencies can use pooled resources from the cloud provider, including storage, processing, memory, and network bandwidth.
- **Rapid elasticity.** Agencies can provision the resources that are allocated to match what actual resources are needed according to demand. This is done by scaling resources up or down by adding or removing processing or memory capacity, or both, according to demand.
- **Measured service.** Agencies can pay for services based on usage. This allows agencies to monitor, control, and generate reports, providing greater transparency into the agency's use of cloud services.

---

## OMB's Mission and Guidance Related to Cloud Computing Services

OMB is tasked with overseeing federal agencies' management of information and information technology, as well as procurement.<sup>8</sup> Within OMB, primary responsibility for oversight of federal IT has been given to the Administrator of the Office of Electronic Government and Information

---

<sup>8</sup>40 U.S.C. § 11302-03 (*Clinger-Cohen Act*); see also 44 U.S.C. § 3504 (*Paperwork Reduction Act*); 44 U.S.C. § 3602 (*E-Government Act*); 44 U.S.C. § 3553 (*Federal Information Security Modernization Act of 2014*, which largely superseded the *Federal Information Security Management Act of 2002*).

---

Technology, who is also called the Federal CIO.<sup>9</sup> As a part of its oversight, OMB develops and ensures the implementation of policies and guidelines that drive enhanced technology performance and budgeting for the federal government.

In December 2010, OMB made cloud computing an integral part of its *25 Point Implementation Plan to Reform Federal Information Technology Management*.<sup>10</sup> The plan called for the development of a government-wide strategy to hasten the adoption of cloud services. To accelerate the shift, OMB required agencies to identify three systems to migrate to cloud services, create a project plan for migration, and migrate all three systems by June 2012.

Subsequently, in February 2011, OMB issued the *Federal Cloud Computing Strategy*, that required each agency's CIO to evaluate safe, secure cloud computing options before making any new investments.<sup>11</sup> The strategy provided definitions of cloud services; benefits of cloud services, such as accelerating data center consolidations; a decision framework for migrating services to a cloud environment;<sup>12</sup> case studies to support agencies' migration to cloud services; and roles and responsibilities for federal agencies.

Further, to facilitate the adoption and use of cloud services, OMB established the Federal Risk and Authorization Management Program (FedRAMP) in 2011. The program is intended to provide a standardized approach for selecting and authorizing the use of cloud services that meet federal security requirements. Managed by GSA, the program aims to ensure that cloud services have adequate information security, while also eliminating duplicative efforts and reducing operational costs. OMB

---

<sup>9</sup>OMB's Office of Electronic Government works with OMB's Office of Information and Regulatory Affairs in carrying out its IT management responsibilities. 44 U.S.C. § 3602.

<sup>10</sup>Office of Management and Budget, *25 Point Implementation Plan to Reform Federal Information Technology Management* (Dec. 9, 2010).

<sup>11</sup>Office of Management and Budget, *Federal Cloud Computing Strategy* (Feb. 8, 2011).

<sup>12</sup>The decision framework, among other things, identified several key areas for determining the readiness for moving to a cloud environment, including the ability of the cloud service provider to address government security requirements.

required all agencies to use FedRAMP for authorizing cloud services by June 2014.<sup>13</sup>

In June 2019, OMB issued an update to its *Federal Cloud Computing Strategy* (Cloud Smart) in an effort to accelerate agency adoption of cloud-based solutions.<sup>14</sup> The strategy focused on equipping agencies with the tools needed to make informed IT decisions according to its mission needs. In addition, the strategy included five key requirements for agencies to address within the area of procurement that were intended to help ensure successful cloud implementation. Table 1 outlines the five key requirements.

**Table 1: Key Procurement Cloud Computing Requirements in OMB’s Cloud Smart Strategy**

Key requirement	Description
Ensure the agency’s chief information officer oversees modernization.	The agency Chief Information Officer should oversee the modernization process.
Iteratively improve agency policies and guidance.	Agencies will need to iteratively improve policies, technical guidance, and business requirements.
Have cloud service level agreement (SLA) in place.	Agencies should have a cloud SLA with vendors that deploy a cloud solution. <sup>a</sup> In the SLA, agencies should ensure they are provided with continuous awareness of the confidentiality, integrity, and availability of its information; should articulate a detailed definition of roles and responsibilities with commercial cloud service providers; establish clear performance metrics with these providers and implement remediation plans for non-compliance.
Standardize cloud contract SLAs.	Agencies must standardize cloud SLAs to provide more effective, efficient, and secure cloud procurement outcomes.
Ensure continuous visibility in high value asset contracts.	Agencies must ensure that contracts affecting their high value assets, including those managed and operated in the cloud, include requirements that provide agencies with continuous visibility of the asset. <sup>b</sup>

Source: GAO analysis of the Office of Management and Budget’s (OMB) June 2019 *Federal Cloud Computing Strategy*. | GAO-24-106137

<sup>a</sup>A service level agreement defines levels of service and performance that the agency expects the contractor to meet. The agency uses the SLA-defined information to measure the effectiveness of its cloud services.

<sup>b</sup>A high value asset is a designation for federal information or a federal information system that processes, stores, or transmits high-value information, is considered vital to an agency fulfilling its primary mission, or serves a critical function in maintaining the security and resilience of the Federal civilian enterprise.

<sup>13</sup>In December 2022, Congress enacted the *FedRAMP Authorization Act* as part of the *James M. Inhofe National Defense Authorization Act for Fiscal Year 2023*, which codified the FedRAMP program. James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, Pub. L. No. 117-263, div. E, title LIX, subtitle C, § 5921(a), 136 Stat. 3449, 3458 (December 23, 2022), codified at 44 U.S.C. §3607-3616.

<sup>14</sup>Office of Management and Budget, *Federal Cloud Computing Strategy* (2019).

---

In addition, the CIO Council developed a list of action items for OMB, GSA, and other agency partners to execute the Cloud Smart strategy.<sup>15</sup> These actions were intended to constitute a work plan aimed at creating and updating programs, policies, and resources that the whole of Government would use to advance the agenda outlined in the Cloud Smart strategy.<sup>16</sup> The CIO Council noted the list of items would continue to evolve and improve upon the strategy using lessons learned during the tasks. Each action item listed on the CIO Council's website also included the current progress made to address the requirement. The action items related to procurement as of June 2024 included:

- **Centralize cloud information.** The Information Technology Category Management and GSA's Cloud Solutions Category Team will work with OMB to contribute to the portal in Action 1 (have a central location to share guidance and best practices on cloud-related topics) to centralize information about cloud initiatives and resources for procurement.<sup>17</sup> Information will include cloud readiness assessment guides, standard requirements, common contract terms and conditions, etc. This action item was listed as complete.
- **Build supplier relationships.** GSA's Cloud Solutions Category Team will implement supplier-relationship management through active engagement with industry partners. Key practices for successful category management include effective supplier-relationship management, managing supplier behavior beyond contract mechanics, and improved performance. This action item was listed as complete.
- **Establish governmentwide cloud solutions category team.** To ensure that all agencies have an opportunity to collaborate, share best practices, and apply cloud-solutions consistently across the Government, the government-wide Information Technology Category

---

<sup>15</sup>The CIO Council is comprised of federal agency CIOs and is the principal interagency forum for improving agency practices related to the design, acquisition, development, modernization, use, sharing, and performance of federal information resources. The Council is chaired by OMB's Deputy Director for Management.

<sup>16</sup>The list of the action items is located on the CIO Council's website at: <https://cloud.cio.gov/strategy/actions/>.

<sup>17</sup>The portal that was developed is called the Cloud Information Center. The center provides a managed collection of cloud computing best practices, guidance, and templates. The website also provides information to assist agencies in identifying and conducting market research on cloud service providers. <https://cic.gsa.gov>.

---

Manager at GSA will establish a government-wide Cloud Solutions Category Team. This action item was listed as complete.

- **Make recommendations for cloud contract vehicles.** The Cloud Solutions Category Team will evaluate and recommend a set of government-wide contract vehicles for cloud services based on a thorough evaluation of each contract. This action item was listed as in progress.
- **Identify cloud management practices.** OMB and the GSA will create or leverage existing, cross-government working groups to identify agency SLAs not addressed by existing commercial industry offerings specific to unique government requirements. Furthermore, they will standardize key indicators and create guidance in line with more modern practices, such as the use of “failure budgets” and cloud architecture principles so that agencies are more aware of how to design and measure the resiliency of their services and other best practices that are related to cloud management practices. This action item was listed as complete.
- **Provide direction to improve data and security in the cloud.** OMB will provide direction to agencies to improve the security and visibility for information systems and data managed in the cloud, beginning with the incorporation of requirements set forth in the updated HVA policy.<sup>18</sup> This action item was listed as complete.

---

## Prior GAO Reports

During the past several years, we reported on federal agencies’ efforts to implement cloud services, and on the progress that oversight agencies have made to help federal agencies in those efforts. For example, in April 2016, we identified 10 key practices that federal and private-sector guidance noted should be included in SLAs in a contract when acquiring IT services through a cloud services provider.<sup>19</sup> We noted that the key practices could help agencies ensure their cloud services were effective, efficient, and secure. Further, given the importance of SLAs in managing million-dollar cloud service contracts, we reported that agencies could

---

<sup>18</sup>In its updated high value asset (HVA) guidance, OMB required agencies to incorporate requirements into all existing and future contracts and service level agreements (SLAs) that enabled the execution of HVA assessments for federal information systems, including cloud-managed services and contractor-owned, contractor-operated systems. All agencies were responsible for the ongoing authorization of their information systems to ensure the accuracy of the information pertaining to the security and privacy posture of their HVAs. Office of Management and Budget, *Strengthening the Cybersecurity of Federal Agencies by enhancing the High Value Asset Program*, M-19-03 (Washington, D.C.: Dec. 10, 2018).

<sup>19</sup>GAO, *Cloud Computing: Agencies Need to Incorporate Key Practices to Ensure Effective Performance*, [GAO-16-325](#) (Washington, D.C.: Apr. 7, 2016).

better protect their interests by incorporating the pertinent practices into their contracts. Table 2 outlines the 10 key practices, which were organized by the following management areas—roles and responsibilities, performance measures, security, and consequences.

**Table 2: Ten Key Practices for a Cloud Computing Service Level Agreement (SLA)**

<b>Roles and responsibilities</b>	
1.	Specify roles and responsibilities of all parties with respect to the SLA, and, at a minimum, include agency and cloud providers.
2.	Define key terms, such as dates and performance.
<b>Performance measures</b>	
3.	Define clear measures for performance by the contractor. Include which party is responsible for measuring performance. Examples of such measures would include <ul style="list-style-type: none"> <li>• Level of service (e.g., service availability—duration the service is to be available to the agency).</li> <li>• Capacity and capability of cloud service (e.g., maximum number of users that can access the cloud at one time and ability of provider to expand services to more users).</li> <li>• Response time (e.g., how quickly cloud service provider systems process a transaction entered by the customer, response time for responding to service outages).</li> </ul>
4.	Specify how and when the agency has access to its own data and networks. This includes how data and networks are to be managed and maintained throughout the duration of the SLA and transitioned back to the agency in case of exit/termination of service.
5.	Specify the following service management requirements: <ul style="list-style-type: none"> <li>• How the cloud service provider will monitor performance and report results to the agency.</li> <li>• When and how the agency, via an audit, is to confirm performance of the cloud service provider.</li> </ul>
6.	Provide for disaster recovery and continuity of operations planning and testing, including how and when the cloud service provider is to report such failures and outages to the agency. In addition, how the provider will remediate such situations and mitigate the risks of such problems from recurring.
7.	Describe any applicable exception criteria when the cloud provider's performance measures do not apply (e.g., during scheduled maintenance or updates).
<b>Security</b>	
8.	Specify metrics the cloud provider must meet in order to show it is meeting the agency's security performance requirements for protecting data (e.g., clearly define who has access to the data and the protections in place to protect the agency's data).
9.	Specify performance requirements and attributes defining how and when the cloud service provider is to notify the agency when security requirements are not being met (e.g., when there is a data breach).
<b>Consequences</b>	
10.	Specify a range of enforceable consequences, such as penalties, for non-compliance with SLA performance measures.

Source: GAO analysis of data from public and private organizations. Reprinted from GAO-16-325. | GAO-24-106137

However, our review of five agencies' (Defense, HHS, DHS, Treasury, and VA) cloud service contracts found that all 10 key practices were not included in these contracts. We therefore made recommendations to the agencies to incorporate these key practices as their contract and SLAs expire. The agencies generally agreed with our recommendations and, to



---

date, all agencies except Treasury have taken action to implement the recommendations.

We also recommended that OMB include all 10 key practices in future guidance to agencies. OMB took action to implement our recommendation. Specifically, in June 2019, OMB issued its *Federal Cloud Computing Strategy*, which incorporated key practices on SLAs that we had identified in our report related to specifying roles and responsibilities for the agency and the cloud services provider and establishing clear performance metrics. Subsequently, in January 2020, OMB staff reported that they had worked with GSA's Cloud Information Center to identify best practices related to SLAs and had made this guidance available to agencies through the Max.gov portal to help improve federal acquisition of cloud-based technologies.

In April 2019, we found that 16 agencies we reviewed had made progress in implementing cloud computing services—namely, they established assessment guidance, performed assessments, and implemented these services—but the extent of their progress varied.<sup>20</sup> In addition, the 16 agencies reported that they had increased their cloud service spending since 2015 and 13 of the 16 agencies had saved \$291 million to date from these services. However, these agencies identified issues in tracking and reporting cloud spending and savings data, including not having consistent processes in place to do so. Agencies also noted that OMB guidance did not require them to explicitly report savings from cloud implementations and, therefore, they had to specifically collect this data to meet GAO's request. As a result of these identified issues, it was likely that agency-reported cloud spending and savings figures were underreported.

We therefore made recommendations to OMB to require agencies to explicitly report, at least on a quarterly basis, the savings and cost avoidance associated with cloud computing investments. We also recommended that the 16 agencies establish a consistent and repeatable mechanism to track savings and cost avoidances from the migration and deployment of cloud services. Fourteen of the sixteen agencies have taken action to implement our recommendation to establish a mechanism to track savings and cost avoidances. As of March 2024, an official from

---

<sup>20</sup>GAO, *Cloud Computing: Agencies Have Increased Usage and Realized Benefits, but Cost and Savings Data Need to Be Better Tracked*, [GAO-19-58](#) (Washington, D.C.: Apr. 4, 2019).

---

---

## Agencies Had Mixed Results in Establishing Guidance for All Key Procurement Requirements Included in OMB's Cloud Smart Strategy

OMB reported that OMB did not intend to take action to address the recommendation. However, we continue to believe that requiring agencies to explicitly report, at least on a quarterly basis, the savings and cost avoidance associated with cloud computing investments, is necessary. Such reporting would help ensure that the Congress and OMB can determine the extent of progress in achieving savings using cloud services.

OMB's Cloud Smart Strategy issued in June 2019, identified ways to help agencies improve their ability to purchase cloud solutions through repeatable practices and shared knowledge of acquisition principles and risk management.<sup>21</sup> For cloud services procurement, OMB set five key requirements for agencies to address:

- Ensure the CIO oversees modernization.
- Iteratively improve agency policies, technical guidance, and business requirements.
- Have a cloud SLA with vendors that deploy a cloud solution.<sup>22</sup> In the SLA, the agency should ensure it is provided with continuous awareness of the confidentiality, integrity, and availability of its information. The agency should also articulate a detailed definition of roles and responsibilities with the commercial cloud service providers. In addition, the agency should establish clear performance metrics and implement remediation plans for non-compliance.
- Standardize cloud SLAs to provide more effective, efficient, and secure cloud procurement outcomes.

---

<sup>21</sup>Office of Management and Budget, *Federal Cloud Computing Strategy* (2019).

<sup>22</sup>A service level agreement defines levels of service and performance that the agency expects the contractor to meet. The agency uses the SLA-defined information to measure the effectiveness of its cloud services. GAO previously described key practices for cloud computing SLAs and identified a lack of cloud service contracting guidance as a primary reason for agency contracts failing to address all key practices. [GAO-16-325](#).

- 
- Ensure that contracts affecting HVAs, including those managed and operated in the cloud, include requirements that provide the agency with continuous visibility of the asset.<sup>23</sup>

Agencies had mixed results in setting policies and guidance that addressed the five key procurement requirements. Specifically, as of July 2024, five of the 24 agencies (Defense, HHS, Interior, State, and NASA) established guidance that fully addressed all five requirements.<sup>24</sup> The remaining 19 agencies addressed some but not all of the requirements. For example, all 24 agencies addressed the requirement related to ensuring the agency CIO oversaw modernization. In addition, 23 of 24 of the agencies addressed the requirement related to iteratively improving agency policies and guidance. However, most of the agencies did not establish guidance that ensured that they had cloud SLAs in place with the cloud providers. In addition, many agencies did not have guidance in place to standardize cloud SLAs with these providers. Further, just over half of the applicable agencies had guidance to include language in contracts for high value assets to ensure the agency had continuous visibility of those assets.<sup>25</sup>

The table below reflects the extent to which each agency had guidance that addressed the five cloud procurement requirements. In addition,

---

<sup>23</sup>A high value asset is a designation for federal information or a federal information system that processes, stores, or transmits high-value information, is considered vital to an agency fulfilling its primary mission, or serves a critical function in maintaining the security and resilience of the Federal civilian enterprise. Office of Management and Budget, M-19-03. In the Cybersecurity and Infrastructure Security Agency's (CISA) guidance, CISA states that having continuous visibility into assets and applications provides the ability to monitor the integrity and security posture of all cloud deployments. CISA's guidance notes that agencies should consider the capabilities offered by their cloud service providers for ensuring visibility into their assets such as security and risk assessments, continuous monitoring and alerting, identity, credential, and access management capabilities, development, security, and operations integration, and artificial intelligence and machine learning security capabilities. Cybersecurity and Infrastructure Security Agency, *Cloud Security Technical Reference Architecture*, Version 2.0 (Washington, D.C.: June 2022).

<sup>24</sup>OMB's Cloud Smart guidance was not specific regarding how agencies should address these requirements. We therefore focused our assessment on whether the 24 agencies had developed policies and other guidance that addressed these requirements. This was because OMB Circular A-130 requires agency Chief Information Officers (CIO) to define policies and processes in sufficient detail for all information resources. Office of Management and Budget, *Managing Information as a Strategic Resource*, Circular A-130 (July 28, 2016).

<sup>25</sup>Six agencies did not have HVAs stored in the cloud, and therefore, we did not assess them against this requirement.

appendix I provides more details on our assessments of the 24 agencies' policies and processes.

**Table 3: Extent to Which Federal Agencies' Guidance Addressed the Five Office of Management and Budget Procurement-Related Cloud Computing Requirements, as of July 2024**

Agency	Ensure the agency's chief information officer oversees modernization.	Iteratively improve agency policies and guidance.	Have cloud service level agreement in place.	Standardize cloud contract service level agreements.	Ensure continuous visibility in high value asset contracts.
Department of Agriculture	●	●	●	○	◐
Department of Commerce	●	●	○	○	●
Department of Defense	●	●	●	●	●
Department of Education	●	●	◐	●	●
Department of Energy	●	●	○	○	○
Department of Health and Human Services	●	●	●	●	●
Department of Homeland Security	●	●	◐	○	●
Department of Housing and Urban Development	●	●	○	○	○
Department of the Interior	●	●	●	●	●
Department of Justice	●	●	◐	●	—
Department of Labor	●	●	○	○	—
Department of State	●	●	●	●	●
Department of Transportation	●	●	○	◐	○
Department of the Treasury	●	●	○	○	—
Department of Veterans Affairs	●	●	◐	○	○
Environmental Protection Agency	●	●	◐	◐	—
General Services Administration	●	●	◐	○	—
National Aeronautics and Space Administration	●	●	●	●	●
National Science Foundation	●	●	◐	○	◐
Nuclear Regulatory Commission	●	●	○	○	○
Office of Personnel Management	●	●	◐	●	●
Small Business Administration	●	○	○	○	●
Social Security Administration	●	●	◐	●	●

Agency	Ensure the agency's chief information officer oversees modernization.	Iteratively improve agency policies and guidance.	Have cloud service level agreement in place.	Standardize cloud contract service level agreements.	Ensure continuous visibility in high value asset contracts.
U.S. Agency for International Development	●	●	◐	○	—
<b>Total number of agencies with requirements addressed</b>	<b>24</b>	<b>23</b>	<b>6</b>	<b>9</b>	<b>11</b>

- = The agency provided guidance that addressed the requirement.
- ◐ = The agency provided guidance that addressed some, but not all of the requirement.
- = The agency did not provide guidance that addressed any of the requirement.
- = The requirement did not apply to the agency as it had no high value assets stored in the cloud.

Source: GAO analysis of agency documentation. | GAO-24-106137

**Agency CIOs should oversee agency modernization processes.** All 24 agencies had guidance that addressed the first procurement-related requirement. In some cases, agencies ensured CIO oversight of modernization through policies that explicitly assigned such responsibility. For example, both Justice’s order on information technology management and NRC’s guidance and management directive on the responsibilities of the Office of the CIO included language that identified roles and responsibilities for the CIO related to modernization activities.

In other cases, policies assigned the CIO responsibility for modernization-related processes. For example, HUD's memo regarding executive order 13833 included language that identified roles and responsibilities for the CIO related to management, governance, and oversight processes for IT. HUD's IT strategic plan also noted that a primary mission function of the CIO's office was to adapt and utilize new technology and a key goal in this area was IT modernization and innovation. In addition, Transportation's guidance on IT management included language that noted the department needed to keep pace with evolving and emerging technologies necessary to transform the use of IT to meet mission needs. The guidance delegated to the CIO roles and responsibilities under OMB Circular A-130 and the Federal Information Technology Acquisition Reform Act,<sup>26</sup> which would include responsibility for modernization activities.

<sup>26</sup>40 U.S.C § 11311-11319.

---

By fulfilling the first procurement-related requirement, the 24 agencies and their CIOs are more likely to find opportunities for enterprise-wide improvement and realize the benefits of cloud services.

**Agencies should iteratively improve their policies and guidance.**

Twenty-three of 24 agencies had guidance to ensure iterative improvements in agency policies, technical guidance, and business requirements, including those related to cloud services. For example, Energy's plan for cloud technology adoption included language that stated its plan would be updated, reviewed, and reapproved by the CIO on an annual basis to reflect modern technologies and updated cybersecurity practices. In addition, OPM's charter on its cloud center of excellence included language that noted the group's efforts were to identify business requirements, develop strategic and tactical guidance and technology standards, and other policies. The charter also noted that the group would be expected to dynamically accommodate new methods and make updates accordingly. Further, SSA's policy on its cloud services vision and strategy included language that stated the policy must be reviewed and updated to reflect the latest developments on a yearly basis with stakeholders.

The remaining agency, SBA, did not have guidance that fully addressed this requirement. Officials from the Office of the CIO at SBA reported that the agency had not developed guidance in this area; instead, it facilitated iterative improvement to its technical guidance and business requirements through its multiple blanket purchase agreements.<sup>27</sup> However, without guidance in place, the risk remains that the agency will not consistently make improvements to their policies and processes to adapt to changes in cloud technology. By establishing guidance to iteratively improve its policies and processes, SBA can minimize the risk of not keeping pace with evolving cloud technology.

---

<sup>27</sup>The Federal Acquisition Regulation states that a blanket purchase agreement is a simplified method of filling anticipated repetitive needs for supplies or services that functions as a charge account, with terms and conditions agreed upon when the agreement is established. A blanket purchase agreement is not a contract; therefore, the government is not obligated to purchase a minimum quantity or dollar amount and the contractor is not obligated to perform until it accepts an order under the purchase agreement.

---

**Agencies should have an SLA that governs the levels of service and performance the agency expects when procuring cloud services from a vendor.** Six of 24 agencies (Agriculture, Defense, HHS, Interior, State, and NASA) had guidance to ensure that all four elements of an adequate cloud SLA were in place for vendor-deployed cloud services. The four elements are continuous awareness of the confidentiality, integrity, and availability of its information, granularly articulated roles and responsibilities, clear performance metrics, and remediation plans for non-compliance. For example, Agriculture's departmental regulation stated that all appropriate offices must coordinate with the Director of the Office of Contracting and Procurement to have an appropriate SLA that included the elements noted by OMB. The regulation also states that systems owners must ensure that SLAs include requirements for providing Agriculture with the proper level of performance, continuous accountability, awareness, and integrity of its IT assets hosted on cloud services. In addition, both Defense's guidance on cloud acquisition and NASA's guidance on cloud procurement best practices addressed all four elements.

Ten of the agencies (Education, DHS, Justice, VA, EPA, GSA, NSF, OPM, SSA, and USAID) had guidance that partially addressed OMB's requirement by including at least one of the four required elements. Specifically, most of the agencies had guidance that included a detailed definition of roles and responsibilities, continuous awareness of information, and performance metrics.<sup>28</sup> However, the majority of the agencies did not have guidance that included language related to remediation plans. Table 4 provides further detail on those agencies with guidance that partially addressed the four elements of an SLA.

---

<sup>28</sup>Agencies' guidance varied in terms of the contract clauses related to the timeframes in which cloud contractors were required to provide the agencies access to their data. Some agencies' guidance noted that contractors should provide continuous access, while other guidance specified that access should be provided when requested, within 1 to 2 days, or within a month. Since OMB's guidance on having continuous awareness of information was not specific regarding an acceptable timeframe for a contractor to provide access, we determined that an allowable time frame was within 2 days.

**Table 4: Coverage of Required Elements by 10 Agencies with Guidance that Partially Addressed Office of Management and Budget’s Requirements for Cloud Service Level Agreements, as of July 2024**

Element	Addressed element	Did not address element
Continuous awareness of the confidentiality, integrity, and availability of information	8	2
Detailed definition of roles and responsibilities	8	2
Establish clear performance metrics	7	3
Implement remediation plans for non-compliance	1	9

Source: GAO analysis of agency service level agreement documentation. | GAO-24-106137

Officials at these agencies provided explanations why their guidance partially met the requirement. For example, an official from EPA’s Office of Acquisition Solutions reported that the agency had not addressed the element of continuous awareness of information because it was unclear how the element aligned with existing federal security guidance. Officials from USAID’s Office of the CIO reported that the agency did not issue additional guidance because it was the agency’s standard practice to have SLAs in place and include, to the degree possible, the elements noted by OMB.

The remaining eight agencies (Commerce, Energy, HUD, Labor, Transportation, Treasury, NRC, and SBA) had not developed guidance to address the requirement. The officials at these agencies provided a variety of explanations as to why they did not have guidance:

- Officials from Commerce’s Office of the CIO stated that SLAs were established by the cloud provider as a standard market practice. Therefore, the agency could use language in the statement of work to require greater awareness of elements like the continuous awareness of information. Commerce officials reported that they had drafted new guidance in June 2024, which was due to be finalized in October 2024.
- Officials from NRC’s Office of the CIO reported that the agency’s cloud team used a standard process to assess potential cloud provider’s SLAs according to specific requirements. NRC officials noted that they prioritized the use of cloud acquisitions using government-wide acquisition contract (GWAC) vehicles that had been



---

designed to provide standardized language and to promote greater consistency in the acquisition of these services.<sup>29</sup>

- SBA officials in the Office of the CIO noted that the agency had included language in their cloud providers' blanket purchase agreements that would limit the ability of the cloud provider to decrease the service levels in the SLA beyond the minimum level established in the purchase agreement. However, SBA provided no documentation to support these activities.
- Officials from Transportation stated that the agency used standard SLAs made available by the cloud vendors.
- Treasury officials reported that they were in the process of drafting guidance to address cloud procurements, which would include guidance on cloud SLAs. Treasury officials said that the guidance was estimated to be finished by October 2024.

Officials from eight of the 18 agencies also stated that additional guidance from GSA and the CIO Council, with OMB's participation, on how to address these elements in agency guidance would be beneficial. According to OMB staff, the agency had provided guidance on SLA practices in the past on the Max.gov portal, but this guidance was removed from the site.<sup>30</sup> In addition, OMB staff noted that guidance related to cloud SLAs was provided to agencies starting in October 2023. Specifically, GSA's Office of Technology Policy issued guidance to agencies on strategic cloud contracting best practices related to infrastructure as a service deployments.<sup>31</sup>

---

<sup>29</sup>A government-wide acquisition contract (GWAC) is an indefinite delivery, indefinite quantity contract that is awarded by agencies for government-wide use to procure an indefinite quantity of IT goods and services for a fixed period of time. These contracts are pre-competed contracts offering a full range of contract types including fixed-price, cost-reimbursement, labor-hour, and time-and-materials, as allowed by each contract, to make agencies' procurement planning easier. Streamlined ordering procedures, as established in the Federal Acquisition Regulation, sec. 16.505, saves agencies time and money - orders can be issued in considerably less time than other types of procurements. OMB designates agencies that may manage and operate government-wide acquisition vehicles under the Clinger-Cohen Act (40 U.S.C. §11302).

<sup>30</sup>To address a prior recommendation we made, OMB worked with GSA's Cloud Information Center to identify best practices related to SLAs, which was made available to agencies through the Max.gov portal in January 2020. [GAO-16-325](#).

<sup>31</sup>General Services Administration Office of Technology Policy and the FinOps Foundation Cloud Acquisition Working Group, *Strategic Cloud (IaaS) Contracting Best Practices* (October 2023).

---

A review of the guidance found that it could be helpful to agencies in beginning to address this requirement but would not address all the elements required by OMB. In particular, the guidance included some examples related to roles and responsibilities, performance metrics, and remediation plans for non-compliance but did not include information related to the element on the continuous awareness of the confidentiality, integrity, and availability of information. In addition, since the guidance was specific to infrastructure as a service cloud deployments, it might not be useful for other types of cloud service deployments like software as a service. Further, since the guidance was issued in October 2023, it is likely that the agencies in our review would not have had time to incorporate it into their guidance by the end of our review. As a result, while this guidance could be helpful to agencies for beginning to address OMB's requirement, agencies could still benefit from some additional guidance and examples related to the four elements, including continuous awareness of information.

The CIO Council, as a forum for improving agency practices, could facilitate the collection of examples of guidance and language from agencies that have met these requirements, particularly in the area of continuous awareness of information. This would provide the agencies with examples to help develop guidance to address the requirement. Accordingly, the 17 agencies could be more informed on how to address the requirement.

Although Treasury did not address this requirement, we previously made a recommendation to the Treasury related to establishing guidance on SLAs.<sup>32</sup> We recommended Treasury incorporate 10 key SLA practices into their guidance—OMB's four required elements were among these key practices. However, as noted in this report, the agency is still in the process of finalizing its guidance. Therefore, we continue to believe this recommendation is appropriate.

**Agencies should standardize cloud contract service level agreements.** Nine of 24 agencies (Defense, Education, HHS, Interior, Justice, State, NASA, OPM, and SSA) had guidance that standardized cloud contract SLAs. Specifically, Interior's statement of work and objective templates both included language that indicated that cloud vendors would be required to meet the agreements and established performance criteria, which included performance availability and

---

<sup>32</sup>[GAO-16-325](#).

---

accessibility requirements. In addition, HHS's cloud adoption strategy noted that each contract requiring cloud services should establish an SLA which should include key practices related to roles and responsibilities, performance measures, security, and consequences. Further, NASA's guidance included a section with standardized language to be included in cloud contracts' statements of work as well as tailored language for specific cloud providers. The standardized clauses were related to federal cloud acquisition best practices such as roles and responsibilities, guaranteed system availability, and penalties for not meeting metrics.

However, 15 out of 24 agencies did not have guidance that fully addressed this requirement. Specifically, two agencies (Transportation and EPA) had guidance that partially addressed the requirement by including some language that should be inserted into all solicitations or contracts, which provided some standardization of SLAs, but did not fully meet the intent of OMB's requirement. The remaining 13 agencies (Agriculture, Commerce, Energy, DHS, HUD, Labor, Treasury, VA, GSA, NSF, NRC, SBA, and USAID) did not have guidance that addressed the requirement.

Officials at one agency reported that they had chosen not to develop standardized SLA guidance. Specifically, officials at GSA's Office of the CIO reported that the agency had relied on guidance related to alignment with FedRAMP rather than creating separate guidance to standardize SLA clauses. Officials stated this was because the CIO's office intended that the agency would use standardized SLAs from its authorized FedRAMP cloud providers to address security requirements. While agencies may choose to use FedRAMP authorization as a performance requirement, standardizing a set of SLA clauses helps to ensure the agency is consistently holding their cloud providers accountable for their service, particularly in areas like privacy that are not part of the FedRAMP control baseline.

Officials at four agencies identified three issues that impacted their ability to develop and implement guidance to standardize SLAs with cloud providers.

- **Cloud service providers' SLAs were effectively non-negotiable.** Officials in the Offices of the CIO at two agencies (Commerce and NRC) reported that it was generally not an option to negotiate the terms of the cloud provider's SLA. For example, Commerce officials reported that, since SLAs were established by the cloud contractors as a standard market practice, the department's ability to negotiate

---

changes was minimal. NRC officials also noted that, because the SLAs were developed by the cloud providers, the agency was not in a position to standardize them.

- **Cloud contract vehicles included pre-negotiated SLAs.** Officials in the Offices of the CIO at two agencies (Transportation and NRC) noted using cloud contract vehicles that did not allow them to modify the SLAs. Transportation officials stated that the agency relied on GSA best in class contract vehicles to procure cloud services, and the terms and conditions of the SLAs were pre-negotiated by GSA.<sup>33</sup> As a result, Transportation officials said that there was not a way to add any additional language into those SLAs, but the officials stated that they thought that the SLAs were sufficient. NRC officials also noted that using GWACs were designed to provide standardized language.
- **Reseller-procured cloud services precluded SLAs.** Officials in the Offices of the CIO at one agency (DHS) reported that, because they procured cloud services through a reseller rather than directly with a cloud provider, they did not establish SLAs.<sup>34</sup> For example, DHS officials reported that many of the agency's contracts for cloud services were with resellers or brokers. The officials said that the cloud providers had advertised service levels with performance metrics and enforcement mechanisms which were set unilaterally by the cloud provider and the agency would not or could not contractually enforce an SLA with the cloud provider.

To help address these issues, OMB sponsored a workshop with federal civilian agencies to facilitate multi-agency negotiations with a government federal cloud provider. The participating agencies developed recommendations on common federal terms, conditions, and pricing related to the licensing of cloud services. The objective of the workshop was to reach an agreement with the cloud provider that was more aligned with the needs of the agencies.

---

<sup>33</sup>Best-in-class is a government-wide designation for acquisition solutions that can be used by multiple agencies and that satisfy key criteria defined by OMB. These contract vehicles include terms and conditions, data collection and reporting requirements that reduce administrative burdens and costs, drive greater transparency, standardize and provide data and analytics to inform business decisions, and begin to eliminate practices that dilute or reduce the government's purchasing power.

<sup>34</sup>Cloud resellers typically procure cloud services from cloud-service providers and resell them to its own customers along with value-added services to help customers manage and operate cloud systems.

---

While we recognize the circumstances that agencies have for negotiations with cloud providers may result in leverage disparities and other factors favoring the providers, we have not been made aware of prohibitions or restrictions on agencies entering into negotiations with those providers. Nevertheless, taking advantage of approaches like OMB's workshop that leverage the strength of the federal government's bulk purchasing power can help to address these challenges.

Officials from six agencies noted that a playbook with examples of standardized language from GSA and the CIO's Council, with OMB's input, would be helpful. The CIO Council could collect and share examples of guidance and contract language related to SLA standardization from agencies that have met these requirements. This would give the 15 agencies examples to help develop guidance to address the requirement, which could enable them to provide more secure cloud procurement outcomes.

Although Treasury did not address this requirement, we previously made a recommendation to the Treasury related to establishing guidance on SLAs.<sup>35</sup> We recommended Treasury incorporate 10 key SLA practices into their guidance as the agency's contract and service level agreements expired, which would address OMB's requirement related to standardizing SLAs. However, as noted in this report, the agency is still in the process of finalizing its guidance. Therefore, we continue to believe this recommendation is appropriate.

**Agencies must ensure cloud contracts affecting HVAs provide continuous visibility of the assets.** Eleven of 18 agencies (Commerce, Defense, Education, HHS, DHS, Interior, State, NASA, OPM, SBA, and SSA) had guidance in place that ensured the continuous visibility of HVAs stored in the cloud.<sup>36</sup> Specifically, Defense's guidance assigned component heads with the responsibility of ensuring contracts included specific requirements that would provide continuous visibility of the identified HVA. In addition, DHS's guidance related to cybersecurity language included requirements for continuous monitoring for acquisitions to ensure visibility of the asset and also noted that this language should be included in all cloud contracts, which would apply to contracts for HVAs. Further, SBA's appendix on cybersecurity language for IT

---

<sup>35</sup>[GAO-16-325](#).

<sup>36</sup>Six agencies did not have HVAs stored in the cloud, and therefore, we did not assess them against this requirement.

---

acquisitions included language that applied to all agency contracts and outlined services that ensured the agency had visibility into its IT systems, including HVAs.

The remaining seven agencies did not have guidance that fully addressed this requirement. Two agencies, Agriculture and NSF, partially addressed this requirement. While Agriculture and NSF had established guidance related to ensuring the continuous visibility of its assets, the agency's guidance did not include language that ensured that it applied to high value asset contracts, as OMB required. The other five agencies (Energy, HUD, Transportation, VA, and NRC) did not have guidance in place.

Agency officials at the five agencies provided several explanations for why they did not have guidance in place.

- Officials from the Office of the CIO at NRC reported that they had included language in their contracts requiring the vendor to be FedRAMP authorized, which would require the vendor to perform continuous monitoring functions that would ensure visibility of the asset. However, the officials noted that their agency did not have corresponding guidance in place in this area.
- Officials at the Office of the CIO at Transportation questioned the need for guidance in this area. Transportation officials reported that the agency relied on standard acquisition practices, which were based on the Federal Acquisition Regulation and other federal guidance, and a business need had not risen for separate processes to support HVAs. The officials stated that they thought there was not a risk that HVAs would be unaddressed. However, without a defined process in place for HVAs, there is a risk that the agency will not consistently ensure this language would be added to all appropriate cloud contracts.
- Officials at VA's Office of the CIO reported that they had guidance in place. However, we reviewed VA's provided documentation and found that these documents did not address OMB's requirement. Specifically, the documents provided were not guidance documents and the sections cited were not relevant to the requirement being assessed. Further details of our assessment are included in Table 20 of appendix I.
- Officials at the Office of the CIO at HUD reported that they were working to develop new guidance. Specifically, the officials reported that they were working with department stakeholders to define specific requirements for continuous visibility of HVAs in cloud contracts and

---

establish clear guidelines for what constitutes adequate visibility. The officials noted that they were also focused on looking at access to monitoring tools, data logs, and audit trails. HUD officials reported that these efforts were anticipated to be completed by March 2025.

- Officials from the Office of the CIO at Energy reported that they were working with HVA owners from component organizations to understand the contracting language used in their procurements to ensure the appropriate focus was placed on HVA asset visibility.

In addition, three of these agency officials also reported that a lack of guidance in this area had contributed to their agencies not being able to address the requirement. The CIO Council could gather examples of guidance and language from agencies that have met this requirement. This would provide the seven agencies with examples to help develop guidance and update their contract language to address the requirement.

---

## Conclusions

In the 5 years since OMB's Cloud Smart strategy was issued, five of the 24 agencies established guidance that fully addressed the five procurement-related requirements included in the strategy. While all agencies established guidance on the authority of their CIOs and most agencies ensured iterative improvements in policies, there were significant differences among the agencies in terms of establishing guidance for the two requirements related to SLAs and the requirement related to ensuring continuous visibility of HVAs. Agencies reported that part of the reason for these shortfalls at 18 agencies was the lack of additional guidance.<sup>37</sup> The CIO Council, by providing examples of guidance from agencies that have met this requirement, could provide agencies useful information to address the requirements.

---

## Recommendations for Executive Action

We are making a total of 47 recommendations—one recommendation to the Federal CIO Council and 46 recommendations to 18 of the 24 Chief Financial Officers Act agencies in our review.

- The CIO Council, working with its chair, the Office of Management and Budget's Deputy Director for Management, should collect and share examples of agency guidance and contract language related to OMB's requirements in the Federal Cloud Computing Strategy on: (1) the four key SLA elements, (2) standardizing SLAs, and (3) ensuring that contracts affecting federal agencies' HVAs, including those

---

<sup>37</sup>Although we identified shortfalls at 19 agencies, we did not make recommendations to the Treasury because we had previously made a recommendation to the agency in the areas noted as part of GAO-16-325.

---

managed and operated in the cloud, include requirements that provide agencies with continuous visibility of the asset. (Recommendation 1)

- The Secretary of Agriculture should ensure that the CIO of Agriculture finalizes its guidance on standardizing cloud SLAs. (Recommendation 2)
- The Secretary of Agriculture should ensure that the CIO of Agriculture finalizes its guidance to require that contracts affecting the agency's high value assets that are managed and operated in the cloud include language that provides the agency with continuous visibility of the asset. (Recommendation 3)
- The Secretary of Agriculture should ensure that the CIO of Agriculture updates its existing contracts for high value assets that are managed and operated in the cloud to meet OMB's requirement once guidance from the CIO Council is available on language that provides the agency with continuous visibility of the asset. If modifying the existing contract is not practical, the agency should incorporate language into the contract that will meet OMB's requirement upon option exercise or issuance of a new award. (Recommendation 4)
- The Secretary of Commerce should ensure that the CIO of Commerce finalizes guidance to put a cloud SLA in place with every vendor when a cloud solution is deployed. The guidance should include language that addresses OMB's four required elements for SLAs, including: continuous awareness of the confidentiality, integrity, and availability of its assets; a detailed description of roles and responsibilities; clear performance metrics; and remediation plans for non-compliance. (Recommendation 5)
- The Secretary of Commerce should ensure that the CIO of Commerce finalizes guidance on standardizing cloud SLAs (Recommendation 6)
- The Secretary of Education should ensure that the CIO of Education updates guidance to put a cloud SLA in place with every vendor when a cloud solution is deployed. The guidance should include language that addresses OMB's required elements for SLAs, including: remediation plans for non-compliance. (Recommendation 7)
- The Secretary of Energy should ensure that the CIO of Energy develops guidance to put a cloud SLA in place with every vendor when a cloud solution is deployed. The guidance should include language that addresses OMB's four required elements for SLAs, including: continuous awareness of the confidentiality, integrity, and availability of its assets; a detailed description of roles and responsibilities; clear performance metrics; and remediation plans for non-compliance. (Recommendation 8)



- 
- The Secretary of Energy should ensure that the CIO of Energy develops guidance regarding standardizing cloud SLAs. (Recommendation 9)
  - The Secretary of Energy should ensure that the CIO of Energy develops guidance to require that contracts affecting the agency's HVAs that are managed and operated in the cloud include language that provides the agency with continuous visibility of the asset. (Recommendation 10)
  - The Secretary of Energy should ensure that the CIO of Energy updates its existing contracts for HVAs that are managed and operated in the cloud to meet OMB's requirement once guidance from the CIO Council is available on language that provides the agency with continuous visibility of the asset. If modifying the existing contract is not practical, the agency should incorporate language into the contract that will meet OMB's requirement upon option exercise or issuance of a new award. (Recommendation 11)
  - The Secretary of Homeland Security should ensure that the CIO of DHS updates its guidance to put a cloud SLA in place with every vendor when a cloud solution is deployed. The guidance should include language that addresses OMB's required elements for SLAs, including: remediation plans for non-compliance. (Recommendation 12)
  - The Secretary of Homeland Security should ensure that the CIO of DHS develops guidance regarding standardizing cloud SLAs. (Recommendation 13)
  - The Secretary of Housing and Urban Development should ensure that the CIO of HUD develops guidance to put a SLA in place with every vendor when a cloud solution is deployed. The guidance should include language that addresses OMB's four required elements for SLAs, including: continuous awareness of the confidentiality, integrity, and availability of its assets; a detailed description of roles and responsibilities; clear performance metrics; and remediation plans for non-compliance. (Recommendation 14)
  - The Secretary of Housing and Urban Development should ensure that the CIO of HUD develops guidance regarding standardizing cloud SLAs. (Recommendation 15)
  - The Secretary of Housing and Urban Development should ensure that the CIO of HUD develops guidance to require that contracts affecting the agency's HVAs that are managed and operated in the cloud include language that provides the agency with continuous visibility of the asset. (Recommendation 16)

- 
- The Secretary of Housing and Urban Development should ensure that the CIO of HUD updates its existing contracts for HVAs that are managed and operated in the cloud to meet OMB's requirement once guidance from the CIO Council is available on language that provides the agency with continuous visibility of the asset. If modifying the existing contract is not practical, the agency should incorporate language into the contract that will meet OMB's requirement upon option exercise or issuance of a new award. (Recommendation 17)
  - The Attorney General of the United States should ensure that the CIO of Justice updates guidance to put a SLA in place with every vendor when a cloud solution is deployed. The guidance should include language that addresses OMB's required elements for SLAs, including: remediation plans for non-compliance. (Recommendation 18)
  - The Secretary of Labor should ensure that the CIO of Labor develops guidance to put a cloud SLA in place with every vendor when a cloud solution is deployed. The guidance should include language that addresses OMB's four required elements for SLAs, including: continuous awareness of the confidentiality, integrity, and availability of its assets; a detailed description of roles and responsibilities; clear performance metrics; and remediation plans for non-compliance. (Recommendation 19)
  - The Secretary of Labor should ensure that the CIO of Labor develops guidance regarding standardizing cloud SLAs. (Recommendation 20)
  - The Secretary of Transportation should ensure that the CIO of Transportation develops guidance to put a cloud SLA in place with every vendor when a cloud solution is deployed. The guidance should include language that addresses OMB's four required elements for SLAs, including: continuous awareness of the confidentiality, integrity, and availability of its assets; a detailed description of roles and responsibilities; clear performance metrics; and remediation plans for non-compliance. (Recommendation 21)
  - The Secretary of Transportation should ensure that the CIO of Transportation updates its guidance regarding standardizing cloud SLAs. (Recommendation 22)
  - The Secretary of Transportation should ensure that the CIO of Transportation develops guidance to require that contracts affecting the agency's high value assets that are managed and operated in the cloud include language that provides the agency with continuous visibility of the asset. (Recommendation 23)

- 
- The Secretary of Transportation should ensure that the CIO of Transportation updates its existing contracts for HVAs that are managed and operated in the cloud to meet OMB's requirement once guidance from the CIO Council is available on language that provides the agency with continuous visibility of the asset. If modifying the existing contract is not practical, the agency should incorporate language into the contract that will meet OMB's requirement upon option exercise or issuance of a new award. (Recommendation 24)
  - The Secretary of Veterans Affairs should ensure that the CIO of VA updates guidance to put a SLA in place with every vendor when a cloud solution is deployed. The guidance should include language that addresses OMB's required elements for SLAs, including: continuous awareness of the confidentiality, integrity, and availability of its assets; a detailed description of roles and responsibilities; and clear performance metrics. (Recommendation 25)
  - The Secretary of Veterans Affairs should ensure that the CIO of VA develops guidance regarding standardizing cloud SLAs. (Recommendation 26)
  - The Secretary of Veterans Affairs should ensure that the CIO of VA develops guidance to require that contracts affecting the agency's HVAs that are managed and operated in the cloud include language that provides the agency with continuous visibility of the asset. (Recommendation 27)
  - The Secretary of Veterans Affairs should ensure that the CIO of VA updates its existing contracts for HVAs that are managed and operated in the cloud to meet OMB's requirement once guidance from the CIO Council is available on language that provides the agency with continuous visibility of the asset. If modifying the existing contract is not practical, the agency should incorporate language into the contract that will meet OMB's requirement upon option exercise or issuance of a new award. (Recommendation 28)
  - The Administrator of EPA should ensure that the CIO of EPA updates guidance to put a cloud SLA in place with every vendor when a cloud solution is deployed. The guidance should include language that addresses OMB's required elements for SLAs, including: continuous awareness of the confidentiality, integrity, and availability of its assets; a detailed description of roles and responsibilities; and remediation plans for non-compliance. (Recommendation 29)
  - The Administrator of EPA should ensure that the CIO of EPA updates guidance regarding standardizing cloud SLAs. (Recommendation 30)

- 
- The Administrator of GSA should ensure that the CIO of GSA updates guidance to put a cloud SLA in place with every vendor when a cloud solution is deployed for the agency. The guidance should include language that addresses OMB's required elements for SLAs, including: remediation plans for non-compliance. (Recommendation 31)
  - The Administrator of GSA should ensure that the CIO of GSA develops guidance regarding standardizing cloud SLAs. (Recommendation 32)
  - The Director of the NSF should ensure that the CIO of NSF updates guidance to put a cloud SLA in place with every vendor when a cloud solution is deployed. The guidance should include language that addresses OMB's required elements for SLAs, including: clear performance metrics and remediation plans for non-compliance. (Recommendation 33)
  - The Director of the NSF should ensure that the CIO of NSF develops guidance regarding standardizing cloud SLAs. (Recommendation 34)
  - The Director of the NSF should ensure that the CIO of NSF updates its guidance to require that contracts affecting the agency's high value assets that are managed and operated in the cloud include language that provides the agency with continuous visibility of the asset. (Recommendation 35)
  - The Director of the NSF should ensure that the CIO of NSF updates its existing contracts for high value assets that are managed and operated in the cloud to meet OMB's requirement once guidance from the CIO Council is available on language that provides the agency with continuous visibility of the asset. If modifying the existing contract is not practical, the agency should incorporate language into the contract that will meet OMB's requirement upon option exercise or issuance of a new award. (Recommendation 36)
  - The Chairman of NRC should ensure that the CIO of NRC develops guidance to put a cloud SLA in place with every vendor when a cloud solution is deployed. The guidance should include language that addresses OMB's four required elements for SLAs, including: continuous awareness of the confidentiality, integrity, and availability of its assets; a detailed description of roles and responsibilities; clear performance metrics; and remediation plans for non-compliance. (Recommendation 37)
  - The Chairman of NRC should ensure that the CIO of NRC develops guidance regarding standardizing cloud SLAs. (Recommendation 38)

- 
- The Chairman of NRC should ensure that the CIO of NRC develops guidance to require that contracts affecting the agency's HVAs that are managed and operated in the cloud include language that provides the agency with continuous visibility of the asset. (Recommendation 39)
  - The Chairman of NRC should ensure that the CIO of NRC updates its existing contracts for HVAs that are managed and operated in the cloud to meet OMB's requirement once guidance from the CIO Council is available on language that provides the agency with continuous visibility of the asset. If modifying the existing contract is not practical, the agency should incorporate language into the contract that will meet OMB's requirement upon option exercise or issuance of a new award. (Recommendation 40)
  - The Director of OPM should ensure that the CIO of OPM updates guidance to put a cloud SLA in place with every vendor when a cloud solution is deployed. The guidance should include language that addresses OMB's required element for SLAs: remediation plans for non-compliance. (Recommendation 41)
  - The Administrator of SBA should ensure that the CIO of SBA develops guidance that requires a periodic review of the agency's policies related to cloud services, including any technical guidance and business requirements, to determine if improvements should be made. (Recommendation 42)
  - The Administrator of SBA should ensure that the CIO of SBA develops guidance to put a cloud SLA in place with every vendor when a cloud solution is deployed. The guidance should include language that addresses OMB's four required elements for SLAs, including: continuous awareness of the confidentiality, integrity, and availability of its assets; a detailed description of roles and responsibilities; clear performance metrics; and remediation plans for non-compliance. (Recommendation 43)
  - The Administrator of SBA should ensure that the CIO of SBA develops guidance regarding standardizing cloud SLAs. (Recommendation 44)
  - The Commissioner of SSA should ensure that the CIO of SSA updates guidance to put a cloud SLA in place with every vendor when a cloud solution is deployed. The guidance should include language that addresses OMB's required elements for SLAs, including: clear performance metrics and remediation plans for non-compliance. (Recommendation 45)

- 
- The Administrator of USAID should ensure that the CIO of USAID updates guidance to put a cloud SLA in place with every vendor when a cloud solution is deployed. The guidance should include language that addresses OMB's required elements for SLAs, including: remediation plans for non-compliance. (Recommendation 46)
  - The Administrator of USAID should ensure that the CIO of USAID develops guidance regarding standardizing cloud SLAs. (Recommendation 47)

---

## Agency Comments and Our Evaluation

We provided a draft of this report to OMB, including the CIO Council, and the 24 Chief Financial Officers Act agencies for their review and comment. The draft report included 52 recommendations to 20 entities (the CIO council and 19 agencies). In responding to our draft report, two agencies (Education and HHS) provided us documentation showing that they had previously addressed five recommendations. We reviewed the newly-provided documentation and confirmed it addressed OMB's requirements and our recommendations. We removed the five recommendations, which are discussed below.

Of the 20 entities to which we made recommendations in the draft report, 14 agencies (Commerce, Energy, HHS, DHS, Labor, VA, EPA, GSA, NSF, NRC, OPM, SBA, SSA, and USAID) agreed with the recommendations, one agency (HUD) did not explicitly agree with our recommendations but provided planned actions and target dates for completion to address them, four entities (Agriculture, CIO Council, Justice, and Transportation) neither agreed or disagreed, and one agency (Education) disagreed with the recommendation.

The following 14 agencies agreed with our recommendations:

- In written comments, reprinted in appendix II, Commerce agreed with our recommendations and enclosed documentation that the department had drafted to address the recommendations. Commerce also requested that we change their ratings of "not addressed" to "partially" or "fully addressed". We reviewed the draft documentation and determined that, once the guidance is finalized, it should address OMB's requirements and our recommendations. However, for the purpose of this report, no change was made to the ratings. Further details of our assessment are included in Table 7 of appendix I.
- In written comments, reprinted in appendix IV, Energy concurred with our recommendations from the draft report and stated that the

---

department would work to address them. Specifically, regarding our recommendation to develop guidance on cloud SLAs, the department stated that it would form a working group to develop guidance that incorporated OMB's four required elements. For the recommendation on standardizing cloud SLAs, Energy stated that the department's Office of the CIO would work with Office of Acquisition Management to develop guidance. Regarding the recommendation to develop guidance for HVA contracts, the department stated that it was still assessing the appropriate mechanism to document the requirement. Further, for the recommendation to update HVA contracts, Energy stated that the Office of the CIO and the Office of Acquisition Management would work to modify these contracts once language from the CIO Council was available.

- In written comments, reprinted in appendix V, HHS concurred with our two recommendations from the draft report and stated that the department had previously taken action to implement them. In addition, HHS provided us supporting documentation that they had not previously provided. Our review of HHS's supporting documentation indicated that these documents addressed the intent of our recommendations. Therefore, we removed the two recommendations from this report and updated the report as appropriate to reflect that HHS had addressed the requirement to ensure continuous visibility in HVA contracts. Further details of our assessment are included in Table 11 of appendix I.
- In written comments, reprinted in appendix VI, DHS concurred with our recommendations and stated that the department would take action to address them. Specifically, regarding our recommendation to update guidance on cloud SLAs, the department stated that it would review its cloud computing practice requirements and strengthen its guidance by ensuring the guidance addressed OMB requirements. For the recommendation related to standardizing cloud SLAs, the department stated that it would create, coordinate, and publish a new cloud services policy that would address the requirement for standardizing SLA language and practices.
- In comments provided via email on July 19, 2024, an Economist in Labor's Office of the Assistant Secretary for Policy stated that the department had reviewed the draft report and concurred with both recommendations. In addition, the official noted that the department's corrective action plan was to draft cloud SLA language that could be tailored to the needs of all cloud-based IT contracts and enforce the use of that language in all future IT contracts involving cloud-based capabilities. Further, the official reported that the department had

---

already initiated these actions and would be submitting artifacts to us in the near future which would directly address the recommendations set forth in the draft report.

- In written comments, reprinted in appendix VIII, VA concurred with our recommendations and stated that the department had guidance in place which addressed them. However, we reviewed VA's provided documentation and found that these documents did not address OMB's requirements regarding SLAs, standardizing SLAs, or ensuring continuous visibility of HVA assets. Specifically, while VA provided one guidance document, the guidance was not relevant to the requirements being assessed. The remaining documents were not guidance documents and the sections cited were also not relevant to the requirements being assessed. Further, the documentation addressed specific cloud providers and did not encompass all cloud providers within the department. Consequently, we believe our four recommendations to VA are still warranted. Further details of our assessment are included in Table 20 of appendix I.
- In written comments, reprinted in appendix IX, EPA concurred with our recommendations and stated that the agency would take action to address our recommendations. Specifically, regarding our recommendation to update guidance on cloud SLAs, EPA stated that it would evaluate the agency's current performance metrics and identify any gaps or improvements required to support the agency's mission. EPA said that new SLA metrics and updates would be negotiated with the service provider and incorporated into existing contracts. For the recommendation related to standardizing cloud SLAs, EPA stated that the agency will evaluate existing metrics across existing contracts to identify standard requirements that have evolved organically and incorporate them into guidance related to cloud statements of work, including security requirements already established. The agency stated that it will also develop guidance, including standardized clauses to be incorporated into all cloud statements of work and recommended language that may be tailored to specific cloud providers.
- In written comments, reprinted in appendix X, GSA agreed with our recommendations and stated that the agency would develop a plan to address them.
- In written comments, reprinted in appendix XI, NSF concurred with our recommendations and stated that the agency was working to further formalize and strengthen guidance for cloud acquisitions to include standardized SLAs and high value asset contract language.



- 
- In written comments, reprinted in appendix XII, NRC accepted our recommendations and noted that these recommendations would help the agency bring its guidance up to speed with current practices in accordance with the Federal Cloud Smart strategy.
  - In written comments, reprinted in appendix XIII, OPM concurred with our recommendation and stated that the agency would issue a policy to provide guidance to address it.
  - In written comments, reprinted in appendix XIV, SBA agreed with our recommendations and stated that the agency would develop guidance to address them.
  - In written comments, reprinted in appendix XV, SSA agreed with our recommendation.
  - In written comments, reprinted in appendix XVI, USAID concurred with our recommendations and stated that the agency would take action to update its policies to address the recommendations.

The following agency did not explicitly agree with our recommendations but provided planned actions and target dates for completion to address them:

- In written comments, reprinted in appendix VII, HUD provided an action plan to address each of our recommendations. The plan included a list of actions the department planned to take and a target date for completion.

The following four agencies did not state whether they agreed or disagreed with our recommendations:

- In comments provided via email on July 22, 2024, an IT Specialist in Agriculture's Office of the CIO stated that the department did not have any additional comments or feedback. (The department had previously provided technical comments on the draft report.)
- In comments provided via email on July 30, 2024, an Assistant General Counsel from OMB's Office of General Counsel stated that OMB was responding on behalf of the CIO Council. The CIO Council stated that it did not object to our recommendation on collecting and sharing SLA examples. The Council noted that it wanted to remind us that while they could and do share best practices and examples, it cannot enforce or compel agencies to share information or take action. We acknowledge the CIO Council's statutory role as the designated principal interagency forum for improving agency practices, including the acquisition of federal government information

---

resources.<sup>38</sup> Our report identified multiple examples of guidance from agencies in our review that met OMB’s requirements related to SLA and HVA practices. As we noted, collecting these examples from agencies—whose CIOs are members of the CIO Council—and sharing them could provide agencies (who have not yet met the requirements) useful information to address them. In doing so, agency CIOs will help to improve these practices across the federal government. Consequently, we continue to believe that our recommendation is still warranted.

- In comments provided via email on July 11, 2024, an Audit Liaison Specialist in Justice’s Audit Liaison Group stated that the department did not have any formal or technical comments on the draft report.
- In comments provided via email on July 16, 2024, a Management Analyst in Transportation’s Office of Audit Relations and Program Improvement stated that the department would not be providing a management response to the draft report.

The following agency disagreed with our recommendation:

- On July 18, 2024, in responding to the draft report, a staff member in Education’s Office of the Secretary stated that the department had previously addressed the requirements related to having a cloud SLA in place, standardizing cloud SLAs, and ensuring continuous visibility of HVAs. In addition, Education provided us additional supporting documentation that they had not previously provided. We reviewed the supporting documentation and determined that Education did have guidance in place at the time of our review to address standardizing cloud SLAs and the continuous visibility of HVAs. We also determined that Education had addressed the element in cloud SLAs related to performance metrics. We updated our assessment in Table 9 of appendix I and removed the three recommendations related to standardizing cloud SLAs (one) and ensuring continuous visibility of HVAs (two). However, we found that the documentation did not address the cloud SLA element related to remediation plans for non-compliance and therefore, the recommendation related to cloud SLAs was still warranted.

Subsequently, in written comments, reprinted in appendix III, on July 23, 2024, Education did not concur with our remaining recommendation and stated that the department had guidance in place which addressed remediation plans for non-compliance. We

---

<sup>38</sup>See Pub. L. No. 107-347, 116 Stat. 2899 (Dec. 17, 2002).

---

reviewed Education's guidance and found that the documentation did not address the requirement. Specifically, while Education provided several examples, the majority of the sections cited were not relevant to the requirement being assessed. There was only one example related to vulnerability remediation that included some consequences for contractors related to establishing plans of action and milestones and the possibility of revocation of the authority to operate.

Remediation plans for non-compliance are developed by agencies to hold cloud providers accountable for non-compliance with SLA performance measures by specifying a range of enforceable consequences or penalties. GSA's guidance on strategic cloud best practices—referenced by OMB staff as SLA guidance—also notes that implementing meaningful penalties clearly incentivizes contractors to maintain a high level of performance.<sup>39</sup> Incorporating consequences for each of its identified performance metrics is necessary to ensure Education's cloud contractors are held accountable for their performance. Consequently, we believe our recommendation to Education is still warranted. Further details of our assessment are included in Table 9 of appendix I.

In addition, the draft report included five agencies to which we did not make recommendations in this report. Of these five agencies, Defense concurred without comment and the other four agencies (Interior, State, Treasury, and NASA) had no comments. We also received technical comments from five agencies (Agriculture, Commerce, Education, HHS, and Transportation), which we have incorporated into the report, as appropriate.

---

As agreed with your office, unless you publicly announce the contents of this report earlier, we plan no further distribution until 10 days from the report date. At that time, we will send copies of this report to the appropriate congressional committees, the Director of the Office of Management and Budget, the Secretaries and agency heads of the departments and agencies in this report, and other interested parties. In addition, this report will also be available at no charge on the GAO website at <https://www.gao.gov>.

If you or your staff have any questions about this report, please contact Carol Harris at (202) 512-4456 or [HarrisCC@gao.gov](mailto:HarrisCC@gao.gov). Contact points for

---

<sup>39</sup>General Services Administration Office of Technology Policy and the FinOps Foundation Cloud Acquisition Working Group, *Strategic Cloud (IaaS) Contracting Best Practices* (October 2023).

---

our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix XVII.

Sincerely,

A handwritten signature in black ink, appearing to read "Carol Harris". The signature is written in a cursive, flowing style with a long horizontal stroke at the end.

Carol Harris  
Director, Information Technology  
Acquisition Management Issues

---

# Appendix I: Analysis of Federal Agencies' Guidance to Address OMB's Procurement-Related Cloud Computing Requirements

---

The Office of Management and Budget's (OMB) *Federal Cloud Computing Strategy*, issued in June 2019, included five key requirements for agencies to address.<sup>1</sup> Table 5 outlines the five key requirements.

**Table 5: Key Procurement Cloud Computing Requirements in OMB's *Federal Cloud Computing Strategy***

Key requirement	Description
Ensure the agency's chief information officer oversees modernization.	The agency Chief Information Officer should oversee the modernization processes.
Iteratively improve agency policies and guidance.	Agencies will need to iteratively improve policies, technical guidance, and business requirements.
Have cloud service level agreement (SLA) in place.	Agencies should have a cloud SLA with vendors that deploy a cloud solution. In the SLA, agencies should ensure they are provided with continuous awareness of the confidentiality, integrity, and availability of its information; should articulate a detailed definition of roles and responsibilities with commercial cloud service providers; establish clear performance metrics with these providers and implement remediation plans for non-compliance.
Standardize cloud contract SLAs.	Agencies must standardize cloud SLAs to provide more effective, efficient, and secure cloud procurement outcomes.
Ensure continuous visibility in high value asset contracts.	Agencies must ensure that contracts affecting their high value assets, including those managed and operated in the cloud, include requirements that provide agencies with continuous visibility of the asset.

Source: GAO analysis of the Office of Management and Budget's (OMB) June 2019 *Federal Cloud Computing Strategy*. | GAO-24-106137

OMB's Cloud Smart guidance was not specific regarding how agencies should address these requirements. We therefore focused our assessment on whether the 24 agencies had developed policies and other guidance that addressed these requirements. This was because OMB Circular A-130 requires agency Chief Information Officers (CIO) to define policies and processes in sufficient detail for all information resources.<sup>2</sup>

---

<sup>1</sup>Office of Management and Budget, *Federal Cloud Computing Strategy* (June 24, 2019).

<sup>2</sup>Office of Management and Budget, *Managing Information as a Strategic Resource*, Circular A-130 (July 28, 2016).

The following discusses in detail our assessment of the 24 agencies' policies and processes and the extent to which each agency addressed OMB's five cloud procurement requirements.

**Table 6: Extent to Which Department of Agriculture Guidance Has Addressed the Five OMB Procurement-Related Cloud Requirements, as of July 2024**

Requirement	Assessment	Summary of assessment
Ensure the agency's chief information officer (CIO) oversees modernization.	Fully addressed	Agriculture's policy on CIO authorities included language that identified roles and responsibilities for the CIO related to modernization activities under IT strategic planning and acquisition.
Iteratively improve agency policies and guidance.	Fully addressed	Agriculture's cloud working group charter stated that the group would meet every other week to provide recommendations to the Office of the CIO and Agriculture's CIO Council. Areas to be discussed included cloud policies, technical guidance and business requirements as part of cloud contract requirements, the department's cloud strategy, DevSecOps, and cloud governance.
Have cloud service level agreement (SLA) in place.	Fully addressed	Agriculture's directive stated that all appropriate offices must coordinate with the Director of the Office of Contracting and Procurement to develop an appropriate SLA that included language related to the continuous visibility of assets, vendor performance measurements, clearly defined roles and responsibilities and remediation for non-compliance.
Standardize cloud contract SLAs.	Not addressed	Agriculture provided a copy of a department directive that referenced areas related to SLAs, but the guidance did not standardize the clauses of agreements as the Office of Management and Budget's (OMB) requirement intended. An Agriculture official from the Digital Infrastructure Services Center reported that the Center had been established as the cloud broker for the department to enable standardization of cloud contracts. However, no documentation from the Center was provided to support these standardization activities. In its agency comments, Agriculture provided a copy of its draft Department Regulation 3650 that stated department SLAs should include language related to cloud providers addressing specific federal laws, OMB requirements, security monitoring, performance measurements, and privacy, among others. However, the regulation was still in draft. An Agriculture official from Office of the CIO's Audit Management Program Team reported that the regulation was due to begin the process for finalization on July 19, 2024, but no date for when the guidance would be finalized was provided. Once this regulation is finalized, it should address OMB's requirement.

Requirement	Assessment	Summary of assessment
Ensure continuous visibility in high value asset contracts.	Partially addressed	Although Agriculture established guidance related to ensuring continuous visibility of its assets, the guidance on blanket ordering agreement security requirements only partially addressed OMB's requirement to ensure continuous visibility in high value asset contracts. Specifically, Agriculture's guidance did not indicate that this language was to be included in high value asset contracts. Agriculture also provided a copy of its draft Department Regulation 3650, which required that department SLAs and acquisition vehicles should include language that allowed Agriculture to have continuous visibility of its assets. The regulation also noted that it applied to all department cloud information systems. However, the regulation was still in draft. An Agriculture official from Office of the CIO's Audit Management Program Team reported that the regulation was due to begin the process for finalization on July 19, 2024, but no date for when the guidance would be finalized was provided. Once the department's regulation is finalized, it should address OMB's requirement.

Legend: Fully addressed: The agency provided guidance that addressed the requirement; Partially addressed: The agency provided guidance that addressed some, but not all of the requirement; Not addressed: The agency did not provide guidance that addressed any of the requirement.

Source: GAO analysis of Department of Agriculture documentation and Office of Management and Budget's June 2019 *Federal Cloud Computing Strategy*. | GAO-24-106137

**Table 7: Extent to Which Department of Commerce Guidance Has Addressed the Five OMB Procurement-Related Cloud Requirements, as of July 2024**

Requirement	Assessment	Summary of assessment
Ensure the agency's chief information officer (CIO) oversees modernization.	Fully addressed	Commerce's order identified CIO roles and responsibilities under the Office of Management and Budget (OMB) Circular A-130, Federal Information Technology Acquisition Reform Act, and Clinger Cohen, which would include responsibility for modernization activities.
Iteratively improve agency policies and guidance.	Fully addressed	Commerce's policy on enterprise cybersecurity stated that annual reviews of the policy, which applies to cloud services, would be performed and updates would be made. In addition, Commerce's checklist related to IT compliance in acquisition included a table with a revision list which noted that the checklist had been updated to include additional technical and business requirements over the past few years.
Have cloud service level agreement (SLA) in place.	Not addressed	Commerce officials in the Office of the CIO stated that the department did not have guidance related to SLAs for cloud solutions deployed by commercial cloud providers. In addition, while the department provided copies of system SLAs, these documents were not department guidance and therefore did not address the requirement. Commerce officials reported that SLAs were established by the cloud provider as a standard market practice. Therefore, the department could use language in the statement of work or performance work statement to require greater awareness of elements like the continuous awareness of information. However, no supporting documentation was provided. During the agency comment time frame, Commerce provided a copy of its draft guidance on Cloud Smart Procurement SLAs that included language related to the continuous awareness of information, roles and responsibilities, performance metrics, and remediations plans for non-compliance. However, the guidance was still in draft. An official from Commerce's Office of the Chief Financial Officer reported that the department was due to finalize the guidance in October 2024. Once this guidance is finalized, it should address OMB's requirement.

Requirement	Assessment	Summary of assessment
Standardize cloud contract SLAs.	Not addressed	<p>Commerce officials in the Office of the CIO stated that the department had not developed standardized SLA language. In addition, while the department provided information regarding two of their component's SLAs, these documents were not department guidance and therefore did not address the requirement. Commerce officials reported that the department did not procure cloud service provider support using direct contracts. Furthermore, the officials stated that the SLAs were established by the cloud provider as a standard market practice and therefore standard or generic SLAs might not be the best solution for each procurement. Officials noted that unique SLAs could be developed at the contract level to provide visibility to integrators' performance. During the agency comment time frame, Commerce provided a copy of its draft guidance on Cloud Smart Procurement SLAs that included language for standardizing SLAs. Specifically, the guidance included language related to several areas including the protection of information, continuous monitoring, data jurisdiction, data retention, and incident handling, among others. However, the guidance was still in draft. An official from Commerce's Office of the Chief Financial Officer reported that the department was due to finalize the guidance in October 2024. Once this guidance is finalized, it should address OMB's requirement.</p>
Ensure continuous visibility in high value asset contracts.	Fully addressed	<p>Commerce's handbook on high value assets includes language that assigns system owners and contracting officers with the responsibility for including provisions in contracts related to security controls and assessments. In addition, Commerce's high value asset handbook and continuous monitoring handbook included language related to requiring continuous monitoring to ensure near real-time operational visibility.</p>

Legend: Fully addressed: The agency provided guidance that addressed the requirement; Partially addressed: The agency provided guidance that addressed some, but not all of the requirement; Not addressed: The agency did not provide guidance that addressed any of the requirement.

Source: GAO analysis of Department of Commerce documentation and Office of Management and Budget's June 2019 *Federal Cloud Computing Strategy*. | GAO-24-106137



**Table 8: Extent to Which Department of Defense Guidance Has Addressed the Five OMB Procurement-Related Cloud Requirements, as of July 2024**

Requirement	Assessment	Summary of assessment
Ensure the agency's chief information officer (CIO) oversees modernization.	Fully addressed	Defense's directive identified the CIO with the responsibility for the department's information enterprise. In addition, the department's digital modernization strategy stated that the Defense CIO was responsible for the department's information enterprise.
Iteratively improve agency policies and guidance.	Fully addressed	Defense's guidance designated the department's CIO as the entity responsible for improving policies to increase program efficiency and effectiveness and managing and overseeing its information enterprise. In addition, the department's documentation related to its cloud strategy did take an iterative approach to improving its policies and guidance. For example, the Defense's new guidance on software modernization builds upon existing department strategies and themes related to software, among other things.
Have cloud service level (SLA) agreement in place.	Fully addressed	Defense's guidance on cloud acquisition identified that SLAs should require continuous monitoring to maintain the security and performance of applications. The guidance also specified that these agreements were to include roles and responsibilities of all parties and clear definition of performance measures conducted by contractors, such as level of service and response time. In addition, contractors were to provide for disaster recovery and continuity of operations planning and testing, including how and when the cloud service provider was to report such failures and outages to the agency.
Standardize cloud contract SLAs level agreements.	Fully addressed	Defense's guidance on cloud acquisition identified standardized language and specific contract clauses that were to be used in SLAs in order to provide effective, efficient, and secure cloud procurement.
Ensure continuous visibility in high value asset contracts.	Fully addressed	Defense's guidance on IT risk management required the categorization of department systems identified as high value assets, including those managed and operated in the cloud. In addition, the guidance assigned component heads with the responsibility of ensuring contracts include specific requirements that would provide continuous visibility of the identified high value asset.

Legend: Fully addressed: The agency provided guidance that addressed the requirement; Partially addressed: The agency provided guidance that addressed some, but not all of the requirement; Not addressed: The agency did not provide guidance that addressed any of the requirement.

Source: GAO analysis of Department of Defense documentation and Office of Management and Budget's (OMB) June 2019 *Federal Cloud Computing Strategy*. | GAO-24-106137

**Table 9: Extent to Which Department of Education Guidance Has Addressed the Five OMB Procurement-Related Cloud Requirements, as of July 2024**

Requirement	Assessment	Summary of assessment
Ensure the agency's chief information officer (CIO) oversees modernization.	Fully addressed	Education's guidance on IT governance and investment management included roles and responsibilities for the CIO related to modernization activities.
Iteratively improve agency policies and guidance.	Fully addressed	Education's guidance on IT governance and investment management included language noting that the policy will be updated and reviewed as necessary to keep pace with changing technical needs.

Requirement	Assessment	Summary of assessment
Have cloud service level agreement (SLA) in place.	Partially addressed	Of the four areas noted by OMB that should be included in a cloud SLA, Education's guidance addressed three of these areas. Specifically, Education's guidance on security and privacy requirements addressed roles and responsibilities, continuous awareness of information, and performance metrics. However, Education's provided examples did not address OMB's requirement regarding remediation plans for non-compliance. Specifically, of the five examples Education provided related to performance measures, only three of these—vulnerability remediation, incident response, and contract initiation and expiration—were a type of performance metric, while the remaining two examples described specific roles and responsibilities for the cloud provider to meet with respect to the areas noted. Further, of the three performance metrics, only one—vulnerability remediation—identified language that could be considered consequences for non-compliance. Education's guidance stated that the unmitigated vulnerability would be added to a plan of action and milestone and the contractor's authority to operate could be revoked if the cloud provider failed to meet department security and privacy requirements. Education's guidance included no language that identified consequences for failure to meet the incident response or protection of data in a cloud environment metrics. The other examples of consequences listed by Education were not tied to specific performance metrics. Education's guidance did identify some consequences for cloud contractors related to vulnerability remediation in the form of plans of action and milestones and the possibility of revocation of the authority to operate. However, it is not clear that those consequences establish the type of meaningful penalties that would incentivize contractors to maintain high performance.
Standardize cloud contract SLA.	Fully addressed	Education's contract regulations requires that a standard clause be inserted into all contracts, which states that contractors will maintain compliance with the department's current guidance on security and privacy requirements. The department's guidance on security and privacy requirements included language for standardizing SLAs related to data protection, zero trust, Federal Risk and Authorization Management Program, executive order compliance and trusted internet connections, among others.
Ensure continuous visibility in high value asset contracts.	Fully addressed	Education's contract regulations requires that a standard clause be inserted into all contracts, which states that contractors will maintain compliance with the department's guidance on security and privacy requirements. The department's guidance on security and privacy requirements states that contractors are required to ensure robust physical and cybersecurity protections are in place for all department high value assets. This includes putting in place capabilities, including continuous monitoring, which will ensure continuous visibility of the asset. The guidance also noted that the language was to be included in all cloud contracts, which would apply to contracts for high value assets.

Legend: Fully addressed: The agency provided guidance that addressed the requirement; Partially addressed: The agency provided guidance that addressed some, but not all of the requirement; Not addressed: The agency did not provide guidance that addressed any of the requirement.

Source: GAO analysis of Department of Education documentation and Office of Management and Budget's June 2019 *Federal Cloud Computing Strategy*. | GAO-24-106137

**Table 10: Extent to Which Department of Energy Guidance Has Addressed the Five OMB Procurement-Related Cloud Requirements, as of July 2024**

Requirement	Assessment	Summary of assessment
Ensure the agency's chief information officer (CIO) oversees modernization.	Fully addressed	Energy's order related to information technology management included language that identified roles and responsibilities for the CIO related to modernization activities.
Iteratively improve agency policies and guidance.	Fully addressed	Energy's plan for cloud technology adoption included language that stated its plan would be updated, reviewed, and reapproved by the CIO on an annual basis to reflect modern technologies and updated cybersecurity practices.
Have cloud service level agreement (SLA) in place.	Not addressed	Energy officials in the Office of the CIO reported that the department had not established guidance that addressed the Office of Management and Budget's (OMB) requirement to have cloud SLAs in place. Energy officials reported that they were working to modify their cloud agreements to address SLAs.
Standardize cloud contract SLAs.	Not addressed	Energy officials in the Office of the CIO reported that the department had not established guidance that addressed OMB's requirement to standardize cloud contract SLAs. Energy officials reported that they were working to modify their cloud agreements to address SLAs.
Ensure continuous visibility in high value asset contracts.	Not addressed	Energy officials in the Office of the CIO reported that the department had not established guidance that addressed OMB's requirement to ensure language is included in contracts for high value assets to ensure the continuous visibility of the asset. Energy officials reported that they were working with high value asset owners from component organizations to understand the contracting language used in their procurements to ensure the appropriate focus was placed on asset visibility.

Legend: Fully addressed: The agency provided guidance that addressed the requirement; Partially addressed: The agency provided guidance that addressed some, but not all of the requirement; Not addressed: The agency did not provide guidance that addressed any of the requirement.

Source: GAO analysis of Department of Energy documentation and Office of Management and Budget's June 2019 *Federal Cloud Computing Strategy*. | GAO-24-106137

**Table 11: Extent to Which Department of Health and Human Services (HHS) Guidance Has Addressed the Five OMB Procurement-Related Cloud Requirements, as of July 2024**

Requirement	Assessment	Summary of assessment
Ensure the agency's chief information officer (CIO) oversees modernization.	Fully addressed	HHS's memo on the department CIO delegating authorities to Division CIOs included language that identified roles and responsibilities related to modernization activities.
Iteratively improve agency policies and guidance.	Fully addressed	HHS's policies related to IT acquisitions and procurements included language that required them to be reviewed every three years from the approval date.
Have cloud service level agreement (SLA) in place.	Fully addressed	Of the four areas noted by the Office of Management and Budget (OMB) that should be included in a cloud SLA, HHS's guidance addressed four of these areas. Specifically, HHS's policy on IT procurements addressed roles and responsibilities, performance metrics, continuous awareness of information, and remediation plans.
Standardize cloud contract SLAs.	Fully addressed	HHS's cloud adoption strategy noted that each contract requiring cloud services should establish an SLA which should include key practices related to roles and responsibilities, performance measures, security, and consequences.
Ensure continuous visibility in high value asset contracts.	Fully addressed	HHS's policy on high value assets (HVA) included language that requires all HVAs to use the department's guidance on information technology procurements when creating or updating HVA-related contracts and acquisition requirements. In addition, HHS's IT procurement guidance required that specific contract clauses should be inserted for all cloud contracts related to security compliance and monitoring, including requirements related to ensuring continuous visibility of assets through continuous monitoring activities.

Legend: Fully addressed: The agency provided guidance that addressed the requirement; Partially addressed: The agency provided guidance that addressed some, but not all of the requirement; Not addressed: The agency did not provide guidance that addressed any of the requirement.

Source: GAO analysis of Department of Health and Human Services documentation and Office of Management and Budget's June 2019 *Federal Cloud Computing Strategy*. | GAO-24-106137

**Table 12: Extent to Which Department of Homeland Security (DHS) Guidance Has Addressed the Five OMB Procurement-Related Cloud Requirements, as of July 2024**

Requirement	Assessment	Summary of assessment
Ensure the agency's chief information officer (CIO) oversees modernization.	Fully addressed	DHS's delegation policy and directive included language that identified roles and responsibilities for the CIO related to modernization activities.
Iteratively improve agency policies and guidance.	Fully addressed	DHS's instruction manual included language that stated directives, instructions and other implementing documents would be reviewed within two years of issuance or last revision.
Have cloud service level agreement (SLA) in place.	Partially addressed	Of the four areas noted by the Office of Management and Budget (OMB) that should be included in a cloud SLA, DHS's guidance addressed three of these areas. Specifically, DHS's policy on its information security program addressed roles and responsibilities while the department's guidance on cybersecurity language addressed performance metrics. DHS's contract language addressed continuous awareness of information. There was no documentation to support that remediation plans for non-compliance had been addressed.
Standardize cloud contract SLAs.	Not addressed	DHS officials in the Office of the CIO reported that the department had not established guidance that addressed OMB's requirement to standardize cloud contract SLAs. DHS officials reported that many of the department's contracts for cloud services were with resellers or brokers and the department would not or could not contractually enforce an SLA with the cloud provider, but using a reseller might be the only available option.
Ensure continuous visibility in high value asset contracts.	Fully addressed	DHS's guidance related to cybersecurity language included requirements for continuous monitoring for acquisitions to ensure visibility of the asset and also noted that this language should be included in all cloud contracts, which would apply to contracts for high value assets.

Legend: Fully addressed: The agency provided guidance that addressed the requirement; Partially addressed: The agency provided guidance that addressed some, but not all of the requirement; Not addressed: The agency did not provide guidance that addressed any of the requirement.

Source: GAO analysis of Department of Homeland Security documentation and Office of Management and Budget's June 2019 *Federal Cloud Computing Strategy*. | GAO-24-106137

**Table 13: Extent to Which Department of Housing and Urban Development (HUD) Guidance Has Addressed the Five OMB Procurement-Related Cloud Requirements, as of July 2024**

<b>Requirement</b>	<b>Assessment</b>	<b>Summary of assessment</b>
Ensure the agency's chief information officer (CIO) oversees modernization.	Fully addressed	HUD's memo included language that identified roles and responsibilities for the CIO related to management, governance, and oversight processes for IT. Further, HUD's IT strategic plan noted that a primary mission function of the CIO's office was to adapt and utilize new technology and a key goal in this area was IT modernization and innovation.
Iteratively improve agency policies and guidance.	Fully addressed	HUD's policy on IT security included language that stated the department's planning policy would periodically update security plans and rules of behavior for HUD users for HUD information systems (including cloud systems).
Have cloud service level agreement (SLA) in place.	Not addressed	HUD provided a copy of its cloud provider's SLA. However, as this document was not department guidance, it could not be used to support that the department had developed guidance in this area.
Standardize cloud contract SLAs.	Not addressed	HUD's guide on project planning and management discussed the need for an SLA and the need to negotiate for the services and service levels provided. However, it did not provide guidance to standardize the content of the SLA as the Office of Management and Budget's (OMB) requirement intended.
Ensure continuous visibility in high value asset contracts.	Not addressed	HUD's guidance on cybersecurity and privacy stated that the contractor should provide security to ensure the availability of HUD data applications. However, there was no language related to ensuring HUD staff had continuous visibility of the system. In addition, the guidance did not mention systems designated as high value assets.

Legend: Fully addressed: The agency provided guidance that addressed the requirement; Partially addressed: The agency provided guidance that addressed some, but not all of the requirement; Not addressed: The agency did not provide guidance that addressed any of the requirement.

Source: GAO analysis of Department of Housing and Urban Development documentation and Office of Management and Budget's June 2019 *Federal Cloud Computing Strategy*. | GAO-24-106137

**Table 14: Extent to Which Department of the Interior Guidance Has Addressed the Five OMB Procurement-Related Cloud Requirements, as of July 2024**

<b>Requirement</b>	<b>Assessment</b>	<b>Summary of assessment</b>
Ensure the agency's chief information officer (CIO) oversees modernization.	Fully addressed	Interior's manual on the Office of the CIO included language that identified roles and responsibilities for the CIO related to modernization activities.
Iteratively improve agency policies and guidance.	Fully addressed	Interior's memo on policy management noted that directives should be reviewed every four years.
Have cloud service level agreement (SLA) in place.	Fully addressed	Interior's contract guidance and addendum spreadsheet addressed all four elements required by the Office of Management and Budget (OMB). In addition, the spreadsheet included several additional SLA metrics in other categories such as service reliability, data management, information security, and service support.
Standardize cloud contract SLAs.	Fully addressed	Interior's statement of work and objective templates included language that indicated that cloud vendors would be required to meet SLAs and performance criteria established, which included performance availability and accessibility requirements.
Ensure continuous visibility in high value asset contracts.	Fully addressed	Interior's memo on contract guidelines included language that described continuous monitoring functions that provided continuous visibility, which met OMB's requirement. In addition, there was text which noted that the language was to be included in every contract, which would include high value asset contracts.

Legend: Fully addressed: The agency provided guidance that addressed the requirement; Partially addressed: The agency provided guidance that addressed some, but not all of the requirement; Not addressed: The agency did not provide guidance that addressed any of the requirement.

Source: GAO analysis of Department of the Interior documentation and Office of Management and Budget's June 2019 *Federal Cloud Computing Strategy*. | GAO-24-106137

**Table 15: Extent to Which Department of Justice Guidance Has Addressed the Five OMB Procurement-Related Cloud Requirements, as of July 2024**

Requirement	Assessment	Summary of assessment
Ensure the agency's chief information officer (CIO) oversees modernization.	Fully addressed	Justice's order on information technology management included language that identified roles and responsibilities for the CIO related to modernization activities
Iteratively improve agency policies and guidance.	Fully addressed	Justice's directive on directives management included language that stated its managers would ensure all directives were kept up to date and would review them within five years of issuance.
Have cloud service level agreement (SLA) in place.	Partially addressed	Of the four areas noted by the Office of Management and Budget (OMB) that should be included in a cloud SLA, Justice's guidance addressed three of these areas. Specifically, Justice's guidance on procurement addressed roles and responsibilities. In addition, Justice's guidance on security of information and systems addressed performance metrics and continuous awareness of information. There was no documentation to support that remediation plans for non-compliance had been addressed.
Standardize cloud contract SLAs.	Fully addressed	Justice's guidance on the security of department information and systems included a section of standardized clauses related to areas such as the confidentiality and non-disclosure of department information, as well as continuous monitoring, contingency planning, supply chain risk management reviews, and incident response.
Ensure continuous visibility in high value asset contracts.	Not applicable	Justice officials in the Office of the CIO reported that the department did not have any high value asset-designated systems using cloud services. As such, we determined OMB's requirement to have guidance in place to ensure continuous visibility in high value asset contracts was not applicable.

Legend: Fully addressed: The agency provided guidance that addressed the requirement; Partially addressed: The agency provided guidance that addressed some, but not all of the requirement; Not addressed: The agency did not provide guidance that addressed any of the requirement; Not applicable: The requirement did not apply to the agency as it had no high value assets stored in the cloud.

Source: GAO analysis of Department of Justice documentation and Office of Management and Budget's June 2019 *Federal Cloud Computing Strategy*. | GAO-24-106137



**Table 16: Extent to Which Department of Labor Guidance Has Addressed the Five OMB Procurement-Related Cloud Requirements, as of July 2024**

<b>Requirement</b>	<b>Assessment</b>	<b>Summary of assessment</b>
Ensure the agency's chief information officer (CIO) oversees modernization.	Fully addressed	Labor's policy on general IT management included language that identified roles and responsibilities for the CIO related to modernization activities.
Iteratively improve agency policies and guidance.	Fully addressed	Labor's cloud services guidance included language that stated the department's policies were reviewed annually and its environment was reviewed routinely.
Have cloud service level agreement (SLA) in place.	Not addressed	Labor officials in the Office of the CIO reported that the department had not established guidance that addressed the Office of Management and Budget's (OMB) requirement to have a cloud SLA in place. The officials reported that the department reviewed all cloud service provider proposals for required SLAs and the standards had to exceed the department's internal established SLAs. Officials also said that the department's cloud providers only provided hosting services and that department staff managed the daily operations of its cloud components.
Standardize cloud contract SLAs.	Not addressed	Labor officials in the Office of the CIO reported that the department had not established guidance that addressed OMB's requirement to standardize cloud contract SLA. Labor officials reported that prior to award, the department reviewed technical acceptability against current department standard SLAs. Officials stated that the department was currently working to establish standardized contract language for SLAs.
Ensure continuous visibility in high value asset contracts.	Not applicable	Labor officials in the Office of the CIO reported that the department did not have any high value asset-designated systems using cloud services. As such, we determined OMB's requirement to have guidance in place to ensure continuous visibility in high value asset contracts was not applicable.

Legend: Fully addressed: The agency provided guidance that addressed the requirement; Partially addressed: The agency provided guidance that addressed some, but not all of the requirement; Not addressed: The agency did not provide guidance that addressed any of the requirement; Not applicable: The requirement did not apply to the agency as it had no high value assets stored in the cloud.

Source: GAO analysis of Department of Labor documentation and Office of Management and Budget's June 2019 *Federal Cloud Computing Strategy*. | GAO-24-106137

**Table 17: Extent to Which Department of State Guidance Has Addressed the Five OMB Procurement-Related Cloud Requirements, as of July 2024**

<b>Requirement</b>	<b>Assessment</b>	<b>Summary of assessment</b>
Ensure the agency's chief information officer (CIO) oversees modernization.	Fully addressed	State's policy in its foreign affairs manual included language that identified roles and responsibilities for the CIO related to modernization activities.
Iteratively improve agency policies and guidance.	Fully addressed	State's foreign affairs manual guidance included language that noted that its guidance would be reviewed annually and updated as requested.
Have cloud service level agreement (SLA) in place.	Fully addressed	State's directive on procurement requirement changes included interim changes to the policy which required the department to include the four elements in its SLAs for new requisition packages and contract renewals.
Standardize cloud contract service level agreements.	Fully addressed	State's directive on procurement requirement changes included interim changes to the policy which required the department to include specific elements in SLAs for new requisition packages and contract renewals.
Ensure continuous visibility in high value asset contracts.	Fully addressed	State's directive on procurement requirement changes included interim changes to the policy which stated that an SLA must include a provision that grants the department continuous visibility of the asset for any high value assets hosted on a cloud infrastructure.

Legend: Fully addressed: The agency provided guidance that addressed the requirement; Partially addressed: The agency provided guidance that addressed some, but not all of the requirement; Not addressed: The agency did not provide guidance that addressed any of the requirement.

Source: GAO analysis of Department of State documentation and Office of Management and Budget's (OMB) June 2019 *Federal Cloud Computing Strategy*. | GAO-24-106137

**Table 18: Extent to Which Department of Transportation Guidance Has Addressed the Five OMB Procurement-Related Cloud Requirements, as of July 2024**

Requirement	Assessment	Summary of assessment
Ensure the agency's chief information officer (CIO) oversees modernization.	Fully addressed	Transportation's guidance on IT management included language that noted the department needed to keep pace with evolving and emerging technologies necessary to transform the use of IT to meet mission needs. The guidance delegated the CIO roles and responsibilities under the Office of Management and Budget's (OMB) Circular A-130 and Federal Information Technology Acquisition Reform Act, which would include responsibility for modernization activities.
Iteratively improve agency policies and guidance.	Fully addressed	Transportation's guidance on IT management included language that assigned responsibility to the Associate CIO for IT policy updates and noted that the Associate CIO would lead a review of the department's guidance on an annual basis.
Have cloud service level agreement (SLA) in place.	Not addressed	Transportation officials in the Office of the CIO reported that the department had not established guidance that addressed OMB's requirement to have a cloud SLA in place. Officials said that all cloud vendors did not provide SLAs and, therefore, these agreements were not always available. As a result, the department has requirements for each vendor evaluated and appropriately addressed at the contract level.
Standardize cloud contract SLAs.	Partially addressed	Transportation's guidance required that a standard clause be inserted into all solicitations, which provided some standardization of contracts but did not fully meet the intent of OMB's requirement to standardize SLAs. Transportation officials in the Office of the CIO stated that the department relied on General Services Administration (GSA) best in class contract vehicles to procure cloud services, and the terms and conditions of the SLAs were pre-negotiated by GSA. As a result, Transportation officials said that there was not a way to add any additional language into those SLAs.
Ensure continuous visibility in high value asset contracts.	Not addressed	Transportation officials in the Office of the CIO reported that the department had not established guidance that addressed OMB's requirement to ensure continuous visibility in high value asset contracts. Transportation officials reported that the department's Office of the Senior Procurement Executive had oversight of the department's procurement policies and a business need had not risen for separate procurement policies, processes, or procedures to support high value assets. The officials noted that the department relied on standard acquisition practices, which were based on the Federal Acquisition Regulation and other federal guidance. However, without a defined process in place, there is a risk that the department will not consistently ensure this language would be added to all appropriate cloud contracts.

Legend: Fully addressed: The agency provided guidance that addressed the requirement; Partially addressed: The agency provided guidance that addressed some, but not all of the requirement; Not addressed: The agency did not provide guidance that addressed any of the requirement.

Source: GAO analysis of Department of Transportation documentation and Office of Management and Budget's June 2019 *Federal Cloud Computing Strategy*. | GAO-24-106137

**Table 19: Extent to Which Department of the Treasury Guidance Has Addressed the Five OMB Procurement-Related Cloud Requirements, as of July 2024**

<b>Requirement</b>	<b>Assessment</b>	<b>Summary of assessment</b>
Ensure the agency's chief information officer (CIO) oversees modernization.	Fully addressed	Treasury's directive included language that identified roles and responsibilities for the CIO related to modernization activities.
Iteratively improve agency policies and guidance.	Fully addressed	Treasury's directive included language that stated department directives and other guidance should be reviewed every five years.
Have cloud service level agreement (SLA) in place.	Not addressed	Treasury officials in the Office of the CIO reported that the department had not yet established guidance that addressed the Office of Management and Budget's (OMB) requirement to have a cloud service level agreement in place. Treasury officials reported that they were in the process of drafting guidance to address cloud procurements, which would include guidance on cloud SLAs. Officials said that the guidance was estimated to be finished by October 2024.
Standardize cloud contract SLAs.	Not addressed	Treasury officials in the Office of the CIO reported that the department had not yet established guidance that addressed OMB's requirement to standardize cloud contract service level agreements. Treasury officials reported that they were in the process of drafting guidance to address cloud procurements, which would include guidance on cloud SLAs. Officials said that the guidance was estimated to be finished by October 2024.
Ensure continuous visibility in high value asset contracts.	Not applicable	Treasury officials in the Office of the CIO reported that the department did not have any high value asset-designated systems using cloud services. As such, we determined OMB's requirement to have guidance in place to ensure continuous visibility in high value asset contracts was not applicable.

Legend: Fully addressed: The agency provided guidance that addressed the requirement; Partially addressed: The agency provided guidance that addressed some, but not all of the requirement; Not addressed: The agency did not provide guidance that addressed any of the requirement; Not applicable: The requirement did not apply to the agency as it had no high value assets stored in the cloud.

Source: GAO analysis of Department of the Treasury documentation and Office of Management and Budget's June 2019 *Federal Cloud Computing Strategy*. | GAO-24-106137

**Table 20: Extent to Which Department of Veterans Affairs (VA) Guidance Has Addressed the Five OMB Procurement-Related Cloud Requirements, as of July 2024**

Requirement	Assessment	Summary of assessment
Ensure the agency's chief information officer (CIO) oversees modernization.	Fully addressed	VA's guide on CIO roles, responsibilities and authorities included language that identified roles and responsibilities for the CIO for modernization activities.
Iteratively improve agency policies and guidance.	Fully addressed	VA's guide on the agency's cloud lifecycle management framework described the step by step process for intake and deployment of applications in the department's cloud environment. It included a revision history which showed that the document underwent iterative improvement in line with Office of Management and Budget (OMB) criteria for this requirement.
Have cloud service level agreement (SLA) in place.	Partially addressed	Of the four areas noted by OMB that should be included in a cloud SLA, VA's guidance addressed one of these areas. Specifically, VA provided a procedure for reimbursements for breaches that specifically dealt with remediation plans for non-compliance. In addition, VA provided documentation for the other three areas—continuous awareness of information, roles and responsibilities, and performance metrics—but the documentation did not support that these areas had been addressed. Regarding the continuous awareness of information element, the department's authorization requirements standard operating procedure required the contractor to maintain documentation such as a configuration management plan, business impact analysis, privacy impact analysis, and other documentation that mentioned continuous monitoring activities. However, the guidance did not define those activities in terms of what the contractor would provide. A screenshot of a dashboard scorecard demonstrated that the department was tracking data on its two main cloud providers, but the documentation did not provide evidence that the department had guidance in place. For roles and responsibilities, VA's two system security plans for the department's two main cloud providers each included a table with a list of names and titles of people assigned to specific roles for cloud activities. However, there was no guidance defining the responsibilities of the parties with respect to the activities documented under the cloud SLAs, including key terms such as dates and performance, which should be defined as part of this process. For performance metrics, of the ten examples VA provided related to performance metrics, none of the examples described performance metrics <sup>a</sup> but instead described controls that were put in place. This included identified controls within VA's two system security plans related to elevated privileges, continuous monitoring program, contingency and incident response personnel, security and privacy control assessments, plans of action and milestones, and its analytics and metrics platform, among others. Further, the documentation addressed specific cloud providers and did not provide guidance for all cloud providers within the department.
Standardize cloud contract SLAs.	Not addressed	VA provided a copy of its authorization requirements standard operating procedure which described the procedures that applied to department cloud systems that were required to obtain an authority to operate. This included technical scans, testing, and documentation requirements for the contractor to meet. While VA's document provided guidance on the authorization package, it does not provide guidance on standardizing language that should be included in every SLA for cloud contractors to meet.

Requirement	Assessment	Summary of assessment
Ensure continuous visibility in high value asset contracts.	Not addressed	VA provided copies of two system security plans for the department's two main cloud providers. Based on the three examples of controls provided by VA related to high value assets for each plan, none of the examples contained guidance which noted that language should be included in cloud contracts to ensure the department had continuous visibility of these assets. The controls identified by VA referenced requirements for the contractor to update plans of action and milestones for high value asset systems monthly. Further, VA provided a document showing the results of continuous monitoring controls tested at one cloud provider. While the document demonstrated controls were in place at one provider, it does not demonstrate that VA had guidance to address the requirement. Further, the documentation addressed specific cloud providers and it was not clear that it provided guidance for all HVA-designated systems within the department.

Legend: Fully addressed: The agency provided guidance that addressed the requirement; Partially addressed: The agency provided guidance that addressed some, but not all of the requirement; Not addressed: The agency did not provide guidance that addressed any of the requirement.

Source: GAO analysis of Department of Veterans Affairs documentation and Office of Management and Budget's June 2019 *Federal Cloud Computing Strategy*. | GAO-24-106137

<sup>a</sup>Performance metrics define clear measures of performance by the contractor. Examples of such measures include level of service (e.g. service availability), how and when the agency has access to its own data and networks, and provides for disaster recovery and continuity of operating planning and testing, including how and when the cloud service provider is to report such failures and outages to the agency.

**Table 21: Extent to Which Environmental Protection Agency (EPA) Guidance Has Addressed the Five OMB Procurement-Related Cloud Requirements, as of July 2024**

Requirement	Assessment	Summary of assessment
Ensure the agency's chief information officer (CIO) oversees modernization.	Fully addressed	EPA's policy on enterprise architecture included language that identified roles and responsibilities for the CIO related to modernization activities.
Iteratively improve agency policies and guidance.	Fully addressed	EPA's policy related to directive review and certification processes included language that stated all directives should be reviewed for content, relevance, and clarity. In addition, based on the directive's timeframes, this action was done annually.
Have cloud service level agreement (SLA) in place.	Partially addressed	Of the four areas noted by the Office of Management and Budget (OMB) that should be included in a cloud SLA, EPA's guidance addressed one of these areas. Specifically, EPA provided baseline SLA guidance documentation that addressed performance metrics. There was no documentation to support that the other three areas—continuous awareness of information, roles and responsibilities, and remediation plans—had been addressed.
Standardize cloud contract SLAs.	Partially addressed	EPA's checklist addendum related to cybersecurity tasks included a table that provided some language to standardize applicable cybersecurity tasks but did not include language in other areas like performance metrics noted by OMB guidance. EPA officials from the Office of Acquisition Solutions reported that the agency standardized metrics related to cybersecurity, but other service level minimums might vary from agreement to agreement.
Ensure continuous visibility in high value asset contracts.	Not applicable	EPA officials reported that the agency did not have any high value asset-designated systems using cloud services. As such, we determined OMB's requirement to have guidance in place to ensure continuous visibility in high value asset contracts was not applicable.

Legend: Fully addressed: The agency provided guidance that addressed the requirement; Partially addressed: The agency provided guidance that addressed some, but not all of the requirement; Not addressed: The agency did not provide guidance that addressed any of the requirement; Not applicable: The requirement did not apply to the agency as it had no high value assets stored in the cloud.

Source: GAO analysis of Environmental Protection Agency documentation and Office of Management and Budget's June 2019 *Federal Cloud Computing Strategy*. | GAO-24-106137

**Table 22: Extent to Which General Services Administration (GSA) Guidance Has Addressed the Five OMB Procurement-Related Cloud Requirements, as of July 2024**

Requirement	Assessment	Summary of assessment
Ensure the agency's chief information officer (CIO) oversees modernization.	Fully addressed	GSA's policy on information technology management included language that identified roles and responsibilities for the CIO related to modernization activities.
Iteratively improve agency policies and guidance.	Fully addressed	GSA's procedural guide on IT security included a revision history that showed it had been revised multiple times and indicated it had been updated to improve the policy to address requirements.
Have cloud service level agreement (SLA) in place.	Partially addressed	Of the four areas noted by the Office of Management and Budget (OMB) that should be included in a cloud SLA, GSA's guidance addressed three of these areas. Specifically, GSA's procedural guide on IT security addressed roles and responsibilities, performance metrics, and continuous awareness of information. There was no documentation to support that remediation plans had been addressed.
Standardize cloud contract SLAs.	Not addressed	GSA officials were unable to provide guidance that addressed OMB's requirement to standardize cloud contract SLAs. The documentation that was provided was not related to SLAs and did not ensure standardization of these agreements within the agency. Officials in GSA's Office of the CIO reported that the agency had relied on guidance related to alignment with Federal Risk and Authorization Management Program (FedRAMP) rather than creating separate guidance to standardize SLA clauses. Specifically, GSA officials from the Office of the CIO noted that the agency's guidance ensured alignment with FedRAMP because the CIO's office intended that the agency would use standardized SLAs from its authorized FedRAMP cloud providers to address security requirements. While agencies may choose to use FedRAMP authorization as a performance requirement, standardizing a set of SLA clauses helps to ensure the agency is consistently holding their cloud providers accountable for their service, particularly in areas like privacy that are not part of the FedRAMP control baseline.
Ensure continuous visibility in high value asset contracts.	Not applicable	GSA officials in the Office of the CIO reported that the agency did not have any high value asset-designated systems using cloud services. As such, we determined OMB's requirement to have guidance in place to ensure continuous visibility in high value asset contracts was not applicable.

Legend: Fully addressed: The agency provided guidance that addressed the requirement; Partially addressed: The agency provided guidance that addressed some, but not all of the requirement; Not addressed: The agency did not provide guidance that addressed any of the requirement; Not applicable: The requirement did not apply to the agency as it had no high value assets stored in the cloud.

Source: GAO analysis of General Services Administration documentation and Office of Management and Budget's June 2019 *Federal Cloud Computing Strategy*. | GAO-24-106137

**Table 23: Extent to Which National Aeronautics and Space Administration (NASA) Guidance Has Addressed the Five OMB Procurement-Related Cloud Requirements, as of July 2024**

<b>Requirement</b>	<b>Assessment</b>	<b>Summary of assessment</b>
Ensure the agency's chief information officer (CIO) oversees modernization.	Fully addressed	NASA's handbook included language that assigned roles and responsibilities to the CIO for modernization activities.
Iteratively improve agency policies and guidance.	Fully addressed	NASA's guidance on directives and charters includes language that stated directives were in effect for a maximum of five years and revisions were made whenever a changed was warranted.
Have cloud service level agreement (SLA) in place.	Fully addressed	NASA's guidance on cloud procurement best practices addressed all four areas noted by OMB that should be included in a cloud SLA.
Standardize cloud contract SLAs.	Fully addressed	NASA's guidance related to cloud service statements of work included a section with standardized clauses for the agency's cloud procurements as well as tailored language for specific cloud providers. The standardized clauses were related to federal cloud acquisition best practices such as roles and responsibilities, guaranteed system availability, and penalties for not meeting metrics.
Ensure continuous visibility in high value asset contracts.	Fully addressed	NASA's guidance on high value asset procedures and its security handbook included language that required these assets to adhere to specific agency security requirements, which would ensure the agency had continuous visibility of its high value assets. In addition, NASA's guidance related to cloud service statements of work included a section with standardized clauses for the agency's cloud procurements related to continuous monitoring requirements.

Legend: Fully addressed: The agency provided guidance that addressed the requirement; Partially addressed: The agency provided guidance that addressed some, but not all of the requirement; Not addressed: The agency did not provide guidance that addressed any of the requirement.

Source: GAO analysis of National Aeronautics and Space Administration documentation and Office of Management and Budget's (OMB) June 2019 *Federal Cloud Computing Strategy*. | GAO-24-106137



**Table 24: Extent to Which National Science Foundation (NSF) Guidance Has Addressed the Five OMB Procurement-Related Cloud Requirements, as of July 2024**

Requirement	Assessment	Summary of assessment
Ensure the agency's chief information officer (CIO) oversees modernization.	Fully addressed	NSF's policy on CIO authorities included language that identified roles and responsibilities for the CIO related to modernization activities.
Iteratively improve agency policies and guidance.	Fully addressed	NSF's policy on cloud services included language that stated its policy on its cloud environment and security would be reviewed every five years.
Have cloud service level agreement (SLA) in place.	Partially addressed	Of the four areas noted by the Office of Management and Budget (OMB) that should be included in a cloud SLA, NSF's guidance addressed two of these areas. Specifically, NSF's policy on cloud service security requirements addressed roles and responsibilities and continuous awareness of information. There was no documentation to support that the other two areas—performance metrics and remediation plans—had been addressed.
Standardize cloud contract SLAs.	Not addressed	NSF officials in the Office of the CIO reported that the agency had not established guidance that addressed OMB's requirement to standardize cloud contract SLAs.
Ensure continuous visibility in high value asset contracts.	Partially addressed	Although NSF established guidance related to ensuring continuous visibility of its assets, the guidance only partially addressed OMB's requirement to ensure continuous visibility in high value asset contracts. Specifically, NSF's guidance did not indicate that this language was to be included in high value asset contracts.

Legend: Fully addressed: The agency provided guidance that addressed the requirement; Partially addressed: The agency provided guidance that addressed some, but not all of the requirement; Not addressed: The agency did not provide guidance that addressed any of the requirement.

Source: GAO analysis of National Science Foundation documentation and Office of Management and Budget's June 2019 *Federal Cloud Computing Strategy*. | GAO-24-106137

**Table 25: Extent to Which Nuclear Regulatory Commission (NRC) Guidance Has Addressed the Five OMB Procurement-Related Cloud Requirements, as of July 2024**

<b>Requirement</b>	<b>Assessment</b>	<b>Summary of assessment</b>
Ensure the agency's chief information officer (CIO) oversees modernization.	Fully addressed	NRC's guidance and management directive on the responsibilities of the Office of the CIO included language that identified roles and responsibilities for the CIO related to modernization activities.
Iteratively improve agency policies and guidance.	Fully addressed	NRC's directive on the Office of the CIO included language that stated the office is responsible for coordinating the development and update of agencywide policies related to IT.
Have cloud service level agreement (SLA) in place.	Not addressed	NRC officials in the Office of the CIO reported that the agency used industry vetted cloud provider SLAs. However, as these documents were not agency guidance, they could not be used to support the agency had developed guidance in this area. NRC officials also noted that they prioritized the use of cloud acquisitions using government-wide acquisition contract vehicles that had been designed to provide standardized language and to promote greater consistency in the acquisition of these services.
Standardize cloud contract SLAs.	Not addressed	NRC officials in the Office of the CIO noted that the agency used industry vetted cloud provider SLAs, as these documents were not agency guidance, they could not be used to support the agency had developed guidance in this area. NRC officials also noted that using government-wide acquisition contract vehicles were designed to provide standardized language.
Ensure continuous visibility in high value asset contracts.	Not addressed	NRC officials in the Office of the CIO noted that the agency used industry vetted cloud provider SLAs, as these documents were not agency guidance, they could not be used to support the agency had developed guidance in this area. NRC officials reported that the agency had included language in their contracts requiring the vendor to be Federal Risk and Authorization Management Program authorized, which would require the vendor to perform continuous monitoring functions that would ensure visibility of the asset.

Legend: Fully addressed: The agency provided guidance that addressed the requirement; Partially addressed: The agency provided guidance that addressed some, but not all of the requirement; Not addressed: The agency did not provide guidance that addressed any of the requirement.

Source: GAO analysis of Nuclear Regulatory Commission documentation and Office of Management and Budget's (OMB) June 2019 *Federal Cloud Computing Strategy*. | GAO-24-106137

**Table 26: Extent to Which Office of Personnel Management (OPM) Guidance Has Addressed the Five OMB Procurement-Related Cloud Requirements, as of July 2024**

<b>Requirement</b>	<b>Assessment</b>	<b>Summary of assessment</b>
Ensure the agency’s chief information officer (CIO) oversees modernization.	Fully addressed	OPM’s policy on reservations and delegation of administrative authority included language that delegated the CIO roles and responsibilities under Office of Management and Budget’s (OMB) Circular A-130, Federal Information Technology Acquisition Reform Act, Clinger Cohen, and the eGov Act, which would include responsibility for modernization activities.
Iteratively improve agency policies and guidance.	Fully addressed	OPM’s charter on its cloud center of excellence included language that noted the group’s efforts was to identify business requirements, develop strategic and tactical guidance and technology standards, and other policies. The charter also noted that the group would be expected to dynamically accommodate new methods and make updates accordingly.
Have cloud service level agreement (SLA) in place.	Partially addressed	Of the four areas noted by OMB that should be included in a cloud SLA, OPM’s guidance addressed three of these areas. Specifically, OPM’s IT contract clauses addressed availability of information and roles and responsibilities. OPM’s guidance on specific provisions and clauses addressed performance metrics. There was no documentation to support that remediation plans had been addressed.
Standardize cloud contract SLAs.	Fully addressed	OPM’s documentation on provisions and clauses included several specific clauses that were relevant to cloud-based systems, including clauses for protecting information, addressing security incidents, performing assessments and security monitoring, as well as addressing supply chain risk management.
Ensure continuous visibility in high value asset contracts.	Fully addressed	OPM’s contracting policy included clauses that provided functionality that met OMB’s requirement to ensure continuous visibility of the asset. In addition, there was text that indicated that this language should be included in all acquisitions, which would apply to high value assets.

Legend: Fully addressed: The agency provided guidance that addressed the requirement; Partially addressed: The agency provided guidance that addressed some, but not all of the requirement; Not addressed: The agency did not provide guidance that addressed any of the requirement.

Source: GAO analysis of Office of Personnel Management documentation and Office of Management and Budget’s June 2019 *Federal Cloud Computing Strategy*. | GAO-24-106137

**Table 27: Extent to Which Small Business Administration (SBA) Guidance Has Addressed the Five OMB Procurement-Related Cloud Requirements, as of July 2024**

<b>Requirement</b>	<b>Assessment</b>	<b>Summary of assessment</b>
Ensure the agency's chief information officer (CIO) oversees modernization.	Fully addressed	SBA's standard operating procedure on CIO authorities included language that identified roles and responsibilities for the CIO related to modernization activities.
Iteratively improve agency policies and guidance.	Not addressed	SBA officials in the Office of the CIO confirmed that the agency had no guidance in place. Officials reported that the agency facilitated iterative improvement to its technical guidance and business requirements through its multiple blanket purchase agreements. However, no supporting documentation was provided.
Have cloud service level agreement (SLA) in place.	Not addressed	SBA officials in the Office of the CIO confirmed that the agency had no guidance in place. The officials reported that the agency had included language in their cloud providers' blanket purchase agreements that would limit the ability of the cloud provider to decrease the service levels in the SLA beyond the minimum level outlined in the purchase agreement. However, no supporting documentation was provided.
Standardize cloud contract SLAs.	Not addressed	SBA officials confirmed that the agency had no guidance in place. The officials reported that the agency had included language in their cloud providers' blanket purchase agreements related to metrics like scalability. However, no supporting documentation was provided.
Ensure continuous visibility in high value asset contracts.	Fully addressed	SBA's appendix on cybersecurity language for IT acquisitions included language that applied to all agency contracts and outlines services that ensured the agency had visibility into its IT systems, including high value assets.

Legend: Fully addressed: The agency provided guidance that addressed the requirement; Partially addressed: The agency provided guidance that addressed some, but not all of the requirement; Not addressed: The agency did not provide guidance that addressed any of the requirement.

Source: GAO analysis of Small Business Administration documentation and Office of Management and Budget's (OMB) June 2019 *Federal Cloud Computing Strategy*. | GAO-24-106137

**Table 28: Extent to Which Social Security Administration (SSA) Guidance Has Addressed the Five OMB Procurement-Related Cloud Requirements, as of July 2024**

<b>Requirement</b>	<b>Assessment</b>	<b>Summary of assessment</b>
Ensure the agency's chief information officer (CIO) oversees modernization.	Fully addressed	SSA's directive on CIO responsibilities included language that identified roles and responsibilities for the CIO related to modernization activities.
Iteratively improve agency policies and guidance.	Fully addressed	SSA's policy on cloud services vision and strategy included language that stated the policy must be reviewed and updated to reflect the latest developments on a yearly basis with stakeholders.
Have cloud service level agreement (SLA) in place.	Partially addressed	Of the four areas noted by the Office of Management and Budget (OMB) that should be included in a cloud SLA, SSA's guidance addressed two of these areas. Specifically, SSA's statement of work for cloud providers addressed the availability of information and roles and responsibilities. SSA guidance on blanket purchase agreements also addressed roles and responsibilities. There was no documentation to support that performance metrics and remediation plans had been addressed.
Standardize cloud contract SLAs.	Fully addressed	SSA's guidance on information security requirements for acquisition includes clauses that provide standardization in several areas such as Federal Risk and Authorization Management Program authorization, availability and continued capability.
Ensure continuous visibility in high value asset contracts.	Fully addressed	SSA's statement on work cloud provider access includes contract language that would ensure the agency had continuous visibility of its assets, which would include high value assets.

Legend: Fully addressed: The agency provided guidance that addressed the requirement; Partially addressed: The agency provided guidance that addressed some, but not all of the requirement; Not addressed: The agency did not provide guidance that addressed any of the requirement.

Source: GAO analysis of Social Security Administration documentation and Office of Management and Budget's June 2019 *Federal Cloud Computing Strategy*. | GAO-24-106137

**Table 29: Extent to Which U.S. Agency for International Development (USAID) Guidance Has Addressed the Five OMB Procurement-Related Cloud Requirements, as of July 2024**

Requirement	Assessment	Summary of assessment
Ensure the agency's chief information officer (CIO) oversees modernization.	Fully addressed	USAID's guidance on the CIO's functions and IT portfolio review included language that identified roles and responsibilities for the CIO related to modernization activities.
Iteratively improve agency policies and guidance.	Fully addressed	USAID's guidance on its automated directive system included language that stated that documents must be regularly reviewed and updated as necessary to be consistent with laws and regulations.
Have cloud service level agreement (SLA) in place.	Partially addressed	Of the four areas noted by the Office of Management and Budget (OMB) that should be included in a cloud SLA, USAID's guidance addressed three of these areas. Specifically, USAID's policy on acquisition and assistance addressed roles and responsibilities, performance metrics, and continuous awareness of information. USAID's other guidance documents generally discussed the inclusion of security or privacy requirements for cloud computing but were not specific to remediation plans. USAID's Office of the CIO reported that the agency did not issue additional guidance because it was the agency's standard practice to have SLAs in place and include, to the degree possible, the elements noted by OMB.
Standardize cloud contract SLAs.	Not addressed	USAID's policy on acquisition and assistance, while it included standardized contract language, stated that the contractor would negotiate service levels with USAID and noted items that would be included in an SLA. USAID's guidance therefore did not standardize its cloud contract SLAs but rather provided a process to negotiate an agreement with the cloud service provider.
Ensure continuous visibility in high value asset contracts.	Not applicable	USAID officials in the Office of the CIO reported that the agency did not have any high value asset-designated systems using cloud services. As such, we determined OMB's requirement to have guidance in place to ensure continuous visibility in high value asset contracts was not applicable.

Legend: Fully addressed: The agency provided guidance that addressed the requirement; Partially addressed: The agency provided guidance that addressed some, but not all of the requirement; Not addressed: The agency did not provide guidance that addressed any of the requirement. Not applicable = The requirement did not apply to the agency as it had no high value assets stored in the cloud.

Source: GAO analysis of U.S. Agency for International Development documentation and Office of Management and Budget's June 2019 *Federal Cloud Computing Strategy*. | GAO-24-106137

# Appendix II: Comments from the Department of Commerce



**UNITED STATES DEPARTMENT OF COMMERCE**  
**Office of the Chief Financial Officer and**  
**Assistant Secretary for Administration**  
Washington, D.C. 20230

July 16, 2024

Carol C. Harris  
Director, Information Technology and Cybersecurity  
U.S. Government Accountability Office  
441 G Street NW Washington, DC 20548

Dear Carol C. Harris:

Thank you for the opportunity to respond to the GAO draft report entitled *Cloud Computing: Agencies Need to Address Key OMB Procurement Requirements* (GAO-24-106137).

While the Department agrees with the recommendation(s), we have enclosed additional supporting documentation for the two areas in which Commerce is currently rated as “not addressed” for GAO’s review in hopes to receive a change in our rating to “partially addressed” or “fully addressed”. Additionally, we have highlighted key information within the additional documentation to assist the GAO team with expediting its review/decision and will prepare a formal action plan upon issuance of GAO’s final report.

If you have any questions, please contact MaryAnn Mausser, Department GAO Audit Liaison, at (202) 482-8120 or [mmausser@doc.gov](mailto:mmausser@doc.gov).

Sincerely,

JEREMY PELTER  
Digitally signed by JEREMY PELTER  
Date: 2024.07.16 17:24:48  
+0400

Jeremy Pelter  
Deputy Assistant Secretary for Administration,  
performing the non-exclusive functions and duties  
of the Chief Financial Officer and Assistant  
Secretary for Administration

Enclosures

**Department of Commerce's Comments on  
GAO Draft Report entitled *Cloud Computing: Agencies Need to Address Key OMB  
Procurement Requirements* (GAO-24-106137)**

The Department of Commerce has reviewed the draft report, and we offer the following comments for the Government Accountability Office's (GAO) consideration.

**General Comments**

To seek potential revised ratings in the two areas in which Commerce is currently rated as "not addressed" in the cloud smart procurement assessment, the Department is submitting additional documentation for review and decision for the following: Draft DOC Guidance on Cloud Smart Procurement Service Level Agreement (SLA). Commerce has highlighted areas within the additional documentation to assist GAO in conducting an expedited review/decision. The two key requirements Commerce is seeking to receive revised ratings are as follows:

1. Agencies must have a standardized cloud Service Level Agreement in place (GAO-24-106137, Page 13, Table 3, Row 2, Column 3), and
2. Agencies must have standardized cloud contract Service Level Agreement in place (GAO-24-106137, Page 13, Table 3, Row 2, Column 4).

The Draft DOC Guidance on Cloud Smart Procurement SLA is designed to serve as an overarching guidance for Departmental cloud smart procurement principles and best practices. A group of subject matter experts (SMEs) were assembled from various areas of Departmental expertise (e.g., the Office of the Chief Information Officer; Enterprise Service – Acquisitions; Office of Acquisition and Management, Policy; Office of Cyber Security and Risk Management; Supply Chain SMEs; and many others) to draft the additional documentation. Subsequently, Commerce believes the draft's additional documentation supports the four required elements for SLAs, which are: a) continuous awareness of the confidentiality, integrity, and availability of its assets, b) a detailed description of roles and responsibilities, c) clear performance metrics (this will vary depending on the specific contract and its requirements prior to posting on a formal solicitation), and d) remediation plans for non-compliance.

In lieu of a sample solicitation similar to a real solicitation on Sam.gov, Commerce's plan is for future cloud service solicitations to follow Appendix E, which is discussed in the draft DOC SLA guide.

**Comments on Recommendations**

GAO made two recommendations to the Department of Commerce in the report.

- **Recommendation 1:** "The Secretary of Commerce should ensure that CIO of Commerce develops guidance to put a cloud SLA in place with every vendor when a cloud solution is deployed. The guidance should include language that addresses OMB's four required elements for SLAs, including: continuous awareness of the confidentiality, integrity, and availability of its assets; a detailed description of roles and responsibilities; clear performance metrics; and remediation plans for non-compliance (Recommendation 5, Page 24)."

**Commerce Response:** The Department of Commerce agrees with this recommendation with the caveat to seek a change in the current rating from "not addressed" to either "partially



---

addressed” or “fully addressed”.

- **Recommendation 2:** “The Secretary of Commerce should ensure that CIO of Commerce develops guidance on standardizing cloud SLAs (Recommendation 6, Page 24).”

**Commerce Response:** The Department of Commerce agrees with this recommendation with the caveat to seek a change in the current rating from “not addressed” to either “partially addressed” or “fully addressed”.

# Appendix III: Comments from the Department of Education



UNITED STATES DEPARTMENT OF EDUCATION  
WASHINGTON, D.C. 20202

July 23, 2024

Ms. Carol Harris  
Director  
Information Technology Acquisition  
Management Issues  
U.S. Government Accountability Office  
441 G Street, NW  
Washington, DC 20548

Dear Ms. Harris:

Thank you for the U.S. Government Accountability Office's (GAO's) robust engagement and providing the U.S. Department of Education (Department) the opportunity to review GAO's draft report titled, "Cloud Computing: Agencies Need to Address Key OMB Procurement Requirements (GAO-24-106137)". We appreciate GAO working collaboratively with the Department to address preliminary findings. We would like to note we view the Department as fully compliant with requirements formulated in the Federal Cloud Computing Strategy including the Service Level Agreement (SLA) section. Please see below our response to the remaining finding.

**Recommendation 7:** The Secretary of Education should ensure that the [Chief Information Officer] CIO of Education updates guidance to put cloud SLAs in place with every vendor when a cloud solution is deployed. The guidance should include language that addresses OMB's required elements for SLAs, including remediation plans for non-compliance.

**Response:** The Department does not concur with this recommendation. The Department has acquisition regulations requiring cloud SLAs to be in place with every contractor/vendor when a cloud solution is used by the Department. Additionally, the Department has addressed remediation plans through multiple defined and operating policies and procedures. Supporting documentation is provided in Attachment A.

We appreciate the opportunity to comment on the draft report and GAO's consideration of our comments as the report is finalized.

Sincerely,

**BRIAN BORDELON**  
Digitally signed by BRIAN  
BORDELON  
Date: 2024.07.23 10:58:19 -0400  
Brian Bordelon  
Acting Chief Information Officer

# Appendix IV: Comments from the Department of Energy



**Department of Energy**  
Washington, DC 20585

July 25, 2024

Carol C. Harris  
Director, Information Technology  
Acquisition Management Issues  
U.S. Government Accountability Office  
441 G Street, NW  
Washington, DC 20548

Dear Carol C. Harris:

The Department of Energy (DOE or Department) appreciates the opportunity to provide a response to the Government Accountability Office's (GAO) draft report titled, GAO Draft Report: *Cloud Computing, Agencies Need to Address Key OMB Procurement Requirements (GAO-24-106137)*. DOE concurs with the four (4) recommendations listed in the report and plans to achieve compliance with the Office of Management and Budget (OMB) requirements where technically feasible by September 30, 2025.

GAO should direct any questions to Steven Brand, Deputy Chief Information Officer for Resource Management, at [Steven.Brand@hq.doe.gov](mailto:Steven.Brand@hq.doe.gov).

Sincerely,

A handwritten signature in black ink, appearing to read "Ann Dunkin".

Ann Dunkin  
Chief Information Officer

Enclosure

MANAGEMENT RESPONSE

GAO Draft Report,

*Cloud Computing, Agencies Need to Address Key OMB Procurement Requirements  
(GAO-24-106137)*

**Recommendation 11:** The Secretary of Energy should ensure that the Chief Information Officer (CIO) of Energy develops guidance to put a cloud Service Level Agreement (SLA) in place with every vendor when a cloud solution is deployed. The guidance should include language that addresses Office of Management and Budget's (OMB) four required elements for SLAs including: continuous awareness of the confidentiality, integrity, and availability of its assets; a detailed description of roles and responsibilities; clear performance metrics; and remediation plans for non-compliance.

**Management Response:** *Concur*

The Office of the CIO (OCIO) and the Office of Acquisition Management will form a working group to develop guidance for a cloud SLA that incorporates OMB's four required elements. The OCIO will consult with the working group regarding the appropriate form and content of the recommended guidance.

**Estimated Completion Date:** March 31, 2025

**Recommendation 12:** The Secretary of Energy should ensure that the CIO of Energy develops guidance regarding standardizing cloud SLAs.

**Management Response:** *Concur*

The OCIO will collaborate with the Office of Acquisition Management to develop guidance for a standardized cloud SLA. The CIO's Cloud Strategy working group, established in March 2024, is currently developing a future-state operating model for OCIO-managed clouds. This effort will provide additional insight that may be used to develop the SLA guidance. The OCIO will consult with the working group regarding the appropriate form and content of the recommended guidance.

**Estimated Completion Date:** March 31, 2025

**Recommendation 13:** The Secretary of Energy should ensure that the CIO of Energy develops guidance to require that contracts affecting the agency's High Value Assets (HVA) that are managed and operated in the cloud include language that provides the agency with continuous visibility of the asset.

**Management Response:** *Concur*

The Department of Energy (DOE) has implemented a strategy that emphasizes the visibility and compliance of the HVAs across DOE. In coordination with HVA owners, the OCIO has prioritized resources and funding to address areas of improvement

---

---

including requirements outlined in OMB Memorandum M-21-31. DOE has applied over \$2.5M of funding in FY24 to address the needs of HVA owners in meeting EL3 requirements outlined in M-21-31. Since February 2024, three of the Department's HVAs have advanced from EL0 to EL1, and two HVAs have advanced from EL1 to EL2. Office of the CIO will continue to work with the Office of Acquisition Management to require DOE contracts affecting HVAs to provide DOE with continuous visibility of the asset. DOE is still assessing the appropriate mechanism to document the requirement.

**Estimated Completion Date:** September 30, 2025

**Recommendation 14:** The Secretary of Energy should ensure that the CIO of Energy updates its existing contracts for HVAs, managed and operated in the cloud, to meet OMB's requirements once guidance from the CIO Council is available on language that provides the agency with continuous visibility of the asset. If modifying the existing contracts is not practical, the agency should incorporate language into the contract that will meet OMB's requirement upon option exercise or issuance of a new award.

***Management Response:*** *Concur*

Once the CIO Council issues guidance, the Office of the CIO and the Office of Acquisition Management will work to modify existing contracts to meet the new guidance or will incorporate it upon option exercise or issuance of a new award.

**Estimated Completion Date:** June 30, 2025

# Appendix V: Comments from the Department of Health and Human Services



DEPARTMENT OF HEALTH & HUMAN SERVICES

OFFICE OF THE SECRETARY

Assistant Secretary for Legislation  
Washington, DC 20201

July 22, 2024

Carol C. Harris  
Director, Information Technology  
Acquisition Management Issues  
U.S. Government Accountability Office  
441 G Street NW  
Washington, DC 20548

Dear Ms. Harris:

Attached are comments on the U.S. Government Accountability Office's (GAO) report entitled, **"CLOUD COMPUTING: Agencies Need to Address Key OMB Procurement Requirements"** (GAO-24-106137).

The Department appreciates the opportunity to review this report prior to publication.

Sincerely,

*Melanie Anne Egorin*

Melanie Anne Egorin, PhD  
Assistant Secretary for Legislation

Attachment

---

---

**TECHNICAL COMMENTS FROM THE DEPARTMENT OF HEALTH & HUMAN SERVICES ON THE GOVERNMENT ACCOUNTABILITY OFFICE'S DRAFT CORRESPONDENCE ENTITLED: CLOUD COMPUTING: AGENCIES NEED TO ADDRESS KEY OMB PROCUREMENT REQUIREMENTS (GAO-24-106137)**

The Department of Health & Human Services (HHS) appreciates opportunity to respond to the draft report.

**Recommendation 15**

The Secretary of Health and Human Services should ensure that the CIO of HHS develops guidance to require that contracts affecting the agency's HVAs that are managed and operated in the cloud include language that provides the agency with continuous visibility of the asset.

**HHS Response**

HHS concurs with this recommendation. HHS has taken action to implement this recommendation and believes it has addressed this recommendation. For example, HHS provided its HHS Policy for Information Technology Procurements – Security and Privacy Language and the HHS Policy on High Value Assets.

**Recommendation 16**

The Secretary of Health and Human Services should ensure that the CIO of HHS updates its existing contracts for HVAs, managed and operated in the cloud, to meet OMB's requirement once guidance from the CIO Council is available on language that provides the agency with continuous visibility of the asset. If modifying the existing contract is not practical, the agency should incorporate language into the contract that will meet OMB's requirement upon option exercise or issuance of a new award.

**HHS Response**

HHS concurs with this recommendation. HHS has taken action to implement this recommendation and believes it has addressed this recommendation. For example, HHS provided its HHS Policy for Information Technology Procurements – Security and Privacy Language and the HHS Policy on High Value Assets.

# Appendix VI: Comments from the Department of Homeland Security

U.S. Department of Homeland Security  
Washington, DC 20528



**Homeland  
Security**

BY ELECTRONIC SUBMISSION

July 19, 2024

Carol Harris  
Director, Information Technology and Cybersecurity  
U.S. Government Accountability Office  
441 G Street, NW  
Washington, DC 20548-0001

Re: Management Response to Draft Report GAO-24-106137, "CLOUD COMPUTING: Agencies Need to Address Key OMB Procurement Requirements"

Dear Ms. Harris:

Thank you for the opportunity to comment on this draft report. The U.S. Department of Homeland Security (DHS, or the Department) appreciates the U.S. Government Accountability Office's (GAO) work in planning and conducting its review and issuing this report.

DHS leadership is pleased to note GAO's positive recognition of the DHS Office of the Chief Information Officer (OCIO) efforts to advance cloud modernization, implement processes that ensure ongoing visibility into high-value contracts, and enhance agency policies and guidance. The Department has demonstrated significant improvement in its Service Level Agreement (SLA) governance, with some Components already using standardized SLA language in programmatic contracts that address the complexities of enterprise-level cloud SLA standardization through partnerships across its information technology (IT), business management, and procurement teams. DHS remains committed to further strengthening its foundational guidance for Cloud Computing technologies which supports the critical services the Department provides to the Nation.

The draft report contained 52 recommendations, including 2 for DHS with which the Department concurs. Enclosed find our detailed response to each recommendation. DHS previously submitted technical comments addressing several accuracy, contextual, and other issues under a separate cover for GAO's consideration, as appropriate.



---

Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions. We look forward to working with you again in the future.

Sincerely,

JIM H CRUMPACKER Digitally signed by JIM H  
CRUMPACKER  
Date: 2024.07.19 10:34:42 -04'00'

JIM H. CRUMPACKER  
Director  
Departmental GAO-OIG Liaison Office

Enclosure

---

**Enclosure: Management Response to Recommendations  
Contained in GAO-24-106137**

GAO recommended that the Secretary of Homeland Security ensure that the CIO [Chief Information Officer] of DHS:

**Recommendation 17:** Updates its guidance to put a cloud SLA in place with every vendor when a cloud solution is deployed. The guidance should include language that addresses OMB's [U.S. Office of Management and Budget] required elements for SLAs, including remediation plans for non-compliance.

**Response:** Concur. OCIO reviews all cloud investments for compliance with cybersecurity criteria. While standard cloud SLA language is not yet enforced, there are some elements of SLA language assessed in the compliance reviews. For instance, standard language for continuous awareness of the confidentiality, integrity, and availability of information is nominally achieved through a "continuous monitoring" clause inserted into contracts. OCIO, in coordination with the DHS Management Directorate Office of Program Accountability and Risk Management and the Office of the Chief Procurement Officer, will review its cloud computing practice requirements and further strengthen its SLA Guidance by ensuring the guidance addresses all OMB-required elements for SLAs and is implemented throughout the Department, as appropriate. Estimated Completion Date (ECD): September 30, 2025.

**Recommendation 18:** Develops guidance regarding standardizing cloud SLAs.

**Response:** Concur. OCIO will create, coordinate, and publish a new Cloud Services policy which will address the requirement for use of the standardized SLA language and practices. In doing this, OCIO will consider the existing cloud SLA standards with SLA language present in the United States Coast Guard procurement processes (which leverages the Department of Defense Security Requirements Guide SLAs), FedRAMP SLA standards, and existing DHS IT Policy procurement standards to identify the Cloud SLA foundational language and cloud SLA gaps, and develop updated enterprise-level guidance. ECD: September 30, 2025.

# Appendix VII: Comments from the Department of Housing and Urban Development



U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT  
WASHINGTON, D.C. 20410-3000

CHIEF INFORMATION OFFICER

July 18, 2024

Carol Harris  
Director, Center for Enhanced Cybersecurity  
U.S. Government Accountability Office  
441 G Street, N.W.  
Washington, DC 20226

Re: Cloud Computing: Agencies Need to Address Key OMB Procurement Requirements  
(GAO-24-106137)

Dear Ms. Harris:

I am pleased to provide the formal response for the U.S. Department of Housing and Urban Development (HUD) to the final report produced by the U.S. Government Accountability Office (GAO) titled, Cloud Computing: Agencies Need to Address Key OMB Procurement Requirements (GAO-24-106137).

The enclosure includes our response, planned actions, and target date to achieve GAO's recommendations.

If you have any questions or require additional information, please contact Paul Scott, Business Change & Integration Officer, Office of the Chief Information Officer, at (202) 402-2354 [paul.a.scott@hud.gov](mailto:paul.a.scott@hud.gov).

Sincerely,

A handwritten signature in black ink, appearing to read "Paul A. Scott".

Paul A. Scott  
Business Change & Integration Officer

Enclosure:  
OCIO Program Management Response for (GAO-24-CIO-2203/106137) Cloud Computing:  
Agencies Need to Address Key OMB Procurement Requirements

[www.hud.gov](http://www.hud.gov)

[espanol.hud.gov](http://espanol.hud.gov)

**OCIO Program Management Response for the  
HUD Response  
GAO-24-CIO-2203/106137: Cloud Computing: Agencies Need to Address Key OMB  
Procurement Requirements**

Recommendations to OCIO	Program Management Response
<p>2) The Secretary of Housing and Urban Development should ensure that the CIO of HUD develops guidance regarding standardizing cloud SLAs.</p>	<p>Standardizing SLAs is crucial to ensuring consistency, clarity, and accountability in our cloud deployments. HUD acknowledges the importance of this initiative. We are committed to developing comprehensive guidance under the Leadership of the HUD Secretary and HUD CIO. The action plan listed below outlines HUD’s commitment to standardizing Cloud SLAs to enhance transparency, mitigate risks, and optimize performance across our Cloud initiatives.</p> <p><b>Action Plan:</b></p> <ul style="list-style-type: none"> <li>• Establish HUD Stakeholder Working Group: <ul style="list-style-type: none"> <li>○ Convene a cross-functional working group consisting of HUD IT, General Counsel, Office of Procurement, and HUD Program Management stakeholders.</li> <li>○ Task the working group with reviewing existing SLAs, identifying common requirements, and drafting standardized SLA templates.</li> </ul> </li> <li>• Develop Standardized SLA Framework: <ul style="list-style-type: none"> <li>○ Collaborate with the working group to develop a standardized SLA framework that incorporates best practices and aligns with Cloud Smart and industry standards.</li> <li>○ Include key elements such as performance metrics, security provisions, roles and responsibilities, and compliance measures.</li> </ul> </li> <li>• Approval and Implementation Strategy: <ul style="list-style-type: none"> <li>○ Present the standardized SLA framework to HUD Senior Leadership and obtain approval for adoption across all cloud deployments within the Agency.</li> <li>○ Develop an implementation strategy that includes training sessions for stakeholders on the new SLA framework and procedures for integrating it into procurement and vendor management processes.</li> </ul> </li> </ul>
<p>3) The Secretary of Housing and Urban Development should ensure that the CIO of HUD develops guidance to require that contracts affecting the agency’s HVAs that are managed and operated in the cloud include</p>	<p><b>Target completion date:</b> March 2025  HUD recognizes the critical importance of maintaining continuous visibility and oversight over our HVAs to ensure their IT security and integrity. Under the guidance of the HUD CIO, we are committed to developing comprehensive</p>

**OCIO Program Management Response for the  
HUD Response  
GAO-24-CIO-2203/106137: Cloud Computing: Agencies Need to Address Key OMB  
Procurement Requirements**

Recommendations to OCIO	Program Management Response
<p>2) The Secretary of Housing and Urban Development should ensure that the CIO of HUD develops guidance regarding standardizing cloud SLAs.</p>	<p>Standardizing SLAs is crucial to ensuring consistency, clarity, and accountability in our cloud deployments. HUD acknowledges the importance of this initiative. We are committed to developing comprehensive guidance under the Leadership of the HUD Secretary and HUD CIO. The action plan listed below outlines HUD’s commitment to standardizing Cloud SLAs to enhance transparency, mitigate risks, and optimize performance across our Cloud initiatives.</p> <p><b>Action Plan:</b></p> <ul style="list-style-type: none"> <li>• Establish HUD Stakeholder Working Group: <ul style="list-style-type: none"> <li>○ Convene a cross-functional working group consisting of HUD IT, General Counsel, Office of Procurement, and HUD Program Management stakeholders.</li> <li>○ Task the working group with reviewing existing SLAs, identifying common requirements, and drafting standardized SLA templates.</li> </ul> </li> <li>• Develop Standardized SLA Framework: <ul style="list-style-type: none"> <li>○ Collaborate with the working group to develop a standardized SLA framework that incorporates best practices and aligns with Cloud Smart and industry standards.</li> <li>○ Include key elements such as performance metrics, security provisions, roles and responsibilities, and compliance measures.</li> </ul> </li> <li>• Approval and Implementation Strategy: <ul style="list-style-type: none"> <li>○ Present the standardized SLA framework to HUD Senior Leadership and obtain approval for adoption across all cloud deployments within the Agency.</li> <li>○ Develop an implementation strategy that includes training sessions for stakeholders on the new SLA framework and procedures for integrating it into procurement and vendor management processes.</li> </ul> </li> </ul>
<p>3) The Secretary of Housing and Urban Development should ensure that the CIO of HUD develops guidance to require that contracts affecting the agency’s HVAs that are managed and operated in the cloud include</p>	<p><b>Target completion date:</b> March 2025  HUD recognizes the critical importance of maintaining continuous visibility and oversight over our HVAs to ensure their IT security and integrity. Under the guidance of the HUD CIO, we are committed to developing comprehensive</p>

**OCIO Program Management Response for the  
HUD Response  
GAO-24-CIO-2203/106137: Cloud Computing: Agencies Need to Address Key OMB  
Procurement Requirements**

Recommendations to OCIO	Program Management Response
language that provides the agency with continuous visibility of the asset.	<p>contractual language that provides the necessary visibility into these assets in the Cloud.</p> <p><b>Action Plan:</b> The following action plan outlines HUD’s commitment to enhancing visibility and oversight of our HVAs in the cloud environment, reflecting our dedication to cybersecurity and risk management.</p> <ol style="list-style-type: none"> <li><b>1. Develop Visibility Requirements:</b> <ul style="list-style-type: none"> <li>o Collaborate with HUD’s General Counsel, Office of Procurement Officers, and the Office of the Chief Information Security Officer (OCISO) to define specific requirements for continuous visibility of HVAs in cloud contracts.</li> <li>o Establish clear guidelines for what constitutes adequate visibility, including access to monitoring tools, data logs, and audit trails.</li> </ul> </li> <li><b>2. Incorporate Language into Contract Templates:</b> <ul style="list-style-type: none"> <li>o Modify existing HUD contract templates or create new templates that include standardized language regarding continuous visibility of HVAs in the cloud.</li> <li>o Ensure the language aligns with best practices in cybersecurity and regulatory compliance, addressing confidentiality, integrity, and availability concerns.</li> </ul> </li> <li><b>3. Training and Implementation Strategy:</b> <ul style="list-style-type: none"> <li>o Conduct training sessions for HUD Procurement staff, IT personnel, and relevant stakeholders on the importance of visibility in cloud contracts and the new contractual requirements.</li> <li>o Implement a phased approach to integrate the new contract language into all agreements affecting HVAs, ensuring compliance across all cloud service providers.</li> </ul> </li> </ol> <p><b>Target completion date:</b> March 2025</p>

**OCIO Program Management Response for the  
HUD Response  
GAO-24-CIO-2203/106137: Cloud Computing: Agencies Need to Address Key OMB  
Procurement Requirements**

Recommendations to OCIO	Program Management Response
<p>4) The Secretary of Housing and Urban Development should ensure that the CIO of HUD updates its existing contracts for HVAs, managed and operated in the cloud, to meet OMB's requirement once guidance from the CIO Council is available on language that provides the agency with continuous visibility of the asset. If modifying the existing contract is not practical, the agency should incorporate language into the contract that will meet OMB's requirement upon option exercise or issuance of a new award.</p>	<p>HUD understands the importance of aligning our contracts with Federal guidelines to ensure robust oversight and security of our assets. HUD's CIO will take proactive steps to implement these updates once guidance from the Federal CIO Council is available. Pending Federal CIO Council guidance, HUD has the following Action Plan for this recommendation.</p> <p><b>Action Plan:</b></p> <ol style="list-style-type: none"> <li>1. <b>Monitor Federal CIO Council Guidance:</b> <ul style="list-style-type: none"> <li>o Establish a mechanism to closely monitor updates and guidance from the Federal CIO Council regarding contractual language for continuous visibility of HVAs in the cloud.</li> <li>o Ensure timely review and analysis of the guidance to identify specific requirements and best practices applicable to our agency.</li> </ul> </li> <li>2. <b>Assess Existing Contracts:</b> <ul style="list-style-type: none"> <li>o Conduct a comprehensive review of existing HUD contracts that involve HVAs managed in the cloud.</li> <li>o Identify HUD contracts that need immediate modification and prioritize them based on risk assessment and contract renewal timelines.</li> </ul> </li> <li>3. <b>Modify Existing Contracts or Include Future Language:</b> <ul style="list-style-type: none"> <li>o For HUD contracts that can be modified: <ul style="list-style-type: none"> <li>▪ Work with HUD General Counsel, Office of Procurement specialists, and OCIO to update the contracts with language that meets OMB's requirements for continuous visibility upon renewal or amendment.</li> </ul> </li> <li>o For HUD contracts where modification is not practical: <ul style="list-style-type: none"> <li>▪ Develop a strategy to include OMB-compliant language during option exercises, contract extensions, or issuance of new awards.</li> </ul> </li> </ul> </li> </ol>

**OCIO Program Management Response for the  
HUD Response  
GAO-24-CIO-2203/106137: Cloud Computing: Agencies Need to Address Key OMB  
Procurement Requirements**

Recommendations to OCIO	Program Management Response
	<ul style="list-style-type: none"> <li>▪ Ensure that future contracts incorporate standardized language for continuous visibility as specified by OMB.</li> </ul> <p><b>4. Implementation and Compliance Monitoring:</b></p> <ul style="list-style-type: none"> <li>○ Develop a timeline and implementation plan for updating contracts and incorporating new language.</li> <li>○ Establish monitoring mechanisms to track compliance with updated contract terms and ensure that all HVAs in the cloud are subject to continuous visibility measures.</li> </ul> <p><b><u>Target completion date:</u></b> March 2025 (Dependent on Federal CIO Council contractual language).</p>



# Appendix VIII: Comments from the Department of Veterans Affairs



DEPARTMENT OF VETERANS AFFAIRS  
WASHINGTON

July 26, 2024

Ms. Carol C. Harris  
Director  
Information Technology and Cybersecurity Issues  
U.S. Government Accountability Office  
441 G Street, NW  
Washington, DC 20548

Dear Ms. Harris:

The Department of Veterans Affairs (VA) has reviewed the Government Accountability Office (GAO) draft report, **Cloud Computing: Agencies Need to Address Key OMB Procurement Requirements** (GAO-24-106137).

The enclosure contains the action plan to address the draft report recommendations. VA appreciates the opportunity to comment on your draft report.

Sincerely,

A handwritten signature in black ink that reads "Margaret B. Kabat".

Margaret B. Kabat, LCSW-C, CCM  
Chief of Staff

Enclosure

Enclosure

Department of Veterans Affairs (VA) Comments to  
Government Accountability Office (GAO) Draft Report  
**Cloud Computing: Agencies Need to Address Key OMB  
Procurement Requirements**  
(GAO-24-106137)

**Recommendation 30:** The Secretary of Veterans Affairs should ensure that the CIO of VA updates guidance to put a SLA in place with every vendor when a cloud solution is deployed. The guidance should include language that addresses OMB's required elements for SLAs, including: continuous awareness of the confidentiality, integrity, and availability of its assets; a detailed description of roles and responsibilities; and clear performance metrics.

**VA Comment:** Concur. The Department of Veterans Affairs (VA) fully complies with all Office of Management and Budget-required elements for service level agreements, including continuous awareness of the confidentiality, integrity, and availability of its assets; a detailed description of roles and responsibilities; and clear performance metrics. VA requires an authority to operate for any software used by VA. Evidence of VA's compliance is included in the supporting documentation for each of the following required elements:

Continuous awareness of the confidentiality, integrity, and availability of assets: relevant guidance is included in VA's enterprise Mission Assurance Support Service Authorization Requirements standard operating procedure (Attachment A). The standard operating procedure applies to authority to operate. Please reference pages 109-126. The requirement for any procurement of cloud software is that it be Federal Risk and Authorization Management Program compliant. Please reference pages 128-144 of the standard operating procedure for VA's requirements. Evidence of compliance is shown in screenshots of metrics, monitoring, and resilience dashboards (Attachment B).

Detailed description of roles and responsibilities: please reference the system security plans for Azure (Attachment C) and Amazon Web Services (Attachments D and E) government clouds within the VA Enterprise Cloud. For VA Enterprise Cloud – Azure please see pages 20-23, with critical roles on page 23. For VA Enterprise Cloud – Amazon Web Services, please see pages 27- 30.

Clear performance metrics: please reference Attachment C for VA Enterprise Cloud – Azure (pages 37, 122, 152, 195-196, 204, 296, and 447-450). Please reference Attachment D for VA Enterprise Cloud – Amazon Web Services (pages 40, 131, 162-164, 206-208, 214, 307, and 464-468).

VA requests closure of the recommendation.

**Recommendation 31:** The Secretary of Veterans Affairs should ensure that the CIO of VA develops guidance regarding standardizing cloud SLAs.

**VA Comment:** Concur. VA complies with the requirement to have guidance in place regarding standardizing cloud service level agreements through VA's authority to

Enclosure

Department of Veterans Affairs (VA) Comments to  
Government Accountability Office (GAO) Draft Report  
**Cloud Computing: Agencies Need to Address Key OMB  
Procurement Requirements**  
(GAO-24-106137)

operate guidance, which is a requirement for any cloud product, platform, or application. Please see Attachment A as supporting evidence. VA requests closure of the recommendation.

**Recommendation 32:** The Secretary of Veterans Affairs should ensure that the CIO of VA develops guidance to require that contracts affecting the agency's HVAs that are managed and operated in the cloud include language that provides the agency with continuous visibility of the asset. (Recommendation 32).

**VA Comment:** Concur. VA has guidance in place to ensure continuous visibility of high value assets that are managed and operated in the cloud. VA implements the requirement through VA's authority to operate guidance, which is a requirement for any cloud product, platform, or application. Continuous visibility requirements for high value assets can be found in the relevant system security plan for each product (Attachments C, D, and E). Please reference Attachment C for VA Enterprise Cloud – Azure (pages 296 and 447-450). Please reference Attachments D and E for VA Enterprise Cloud – Amazon Web Services (pages 307 and 464-468). VA requests closure of the recommendation.

**Recommendation 33:** The Secretary of Veterans Affairs should ensure that the CIO of VA updates its existing contracts for HVAs, managed and operated in the cloud, to meet OMB's requirements once guidance from the CIO Council is available on language that provides the agency with continuous visibility of the asset. If modifying the existing contract is not practical, the agency should incorporate language into the contract that will meet OMB's requirement upon option exercise or issuance of a new award.

**VA Comment:** Concur. VA has guidance in place to ensure continuous visibility of high value assets that are managed and operated in the cloud. VA implements the requirement through VA's authority to operate guidance, which is a requirement for any cloud product, platform, or application. Please see the supporting documentation provided for recommendation 32. VA requests closure of the recommendation.

# Appendix IX: Comments from the Environmental Protection Agency



## OFFICE OF MISSION SUPPORT

WASHINGTON, D.C. 20460

July 8, 2024

Ms. Carol C. Harris  
Director  
Information Technology and Cybersecurity  
U.S. Government Accountability Office  
Washington, D.C. 20548

Dear Ms. Harris:

Thank you for the opportunity to review and comment on GAO's draft report, "CLOUD COMPUTING: Agencies Need to Address Key OMB Procurement Requirements" (GAO-24-106137). Following is a summary of the agency's overall position, along with its position on each of the report's recommendations.

### **SUMMARY AND AGENCY'S OVERALL POSITION**

GAO found that agencies had mixed results in setting policies and guidance that addressed the five key procurement requirements established by the Office of Management and Budget (OMB) in its 2019 Cloud Smart Strategy. As of May 2024, all 24 agencies established guidance in place to improve their policies and guidance related to cloud services. However, most agencies did not establish guidance related to service level agreements (SLA).

The agency concurs with the two recommendations.

### **AGENCY'S RESPONSE TO DRAFT RECOMMENDATIONS**

**Recommendation 34:** *The Administrator of EPA should ensure that the CIO of EPA updates guidance to put a cloud SLA in place with every vendor when a cloud solution is deployed. The guidance should include language that addresses OMB's required elements for SLAs, including: continuous awareness of the confidentiality, integrity, and availability of its assets; a detailed description of roles and responsibilities; and remediation plans for non-compliance.*

**EPA Response to Recommendation 34:** EPA generally agrees with the assessment of the EPA cloud program as it relates to executing Service Level Agreements (SLAs) for cloud contracts. EPA has defined the requirements and attributes of service level agreement metrics. However, these requirements have not been incorporated explicitly into cloud contracts with measurable service levels.

EPA incorporates these specific requirements and attributes within security documentation that is compliant with Federal Information Security Modernization Act (FISMA) requirements. Security and contract documentation include roles and responsibilities of both the agency and cloud providers, key terms and conditions required for the contract's performance, and associated dates. Security and contract documentation incorporate these requirements and attributes through terms requiring the provider to meet EPA and Federal policies and procedures. These statements apply to all services provided through the contract, not just cloud services.

The security documentation includes requirements and attributes to ensure the service provider is meeting the agency's security performance requirements including, for example, Maximum Tolerable Downtime (MTD), Recovery Time Objective (RTO) and Recovery Point Objective (RPO) associated with the cloud system. This documentation is maintained by security personnel and reviewed/updated per FISMA requirements.

Consequences for noncompliance with SLA performance measures are incorporated into the overall services contract and are enforceable through the issuance of Award Fees. Penalties for non-compliance with SLA performance include reductions of Award Fees, which incentivize the vendor to maintain compliance.

The EPA will evaluate current performance metrics and assess suitability to EPA requirements. EPA will then cross reference agency contracts and security documentation against cloud service providers' established service level metrics to identify gaps or improvements required to support EPA's mission. New service level metrics and updates will be negotiated with the service provider and incorporated into existing contracts via modification of existing contracts at renewal or at contract establishment with implementation timeframes not to exceed one year. Compliance with established service level requirements and metrics will be monitored and reviewed in accordance with contract review requirements, but not more than once a year.

**Recommendation 35:** *The Administrator of EPA should ensure that the CIO of EPA updates guidance regarding standardizing cloud SLAs.*

**EPA Response to Recommendation 35:** EPA agrees with the assessment of standardized cloud contract service level agreement. EPA has established some language to standardize applicable cybersecurity tasks but needs to develop guidance related to cloud service statements of work and standardize this guidance across cloud providers. Complexities associated with diverse environments, interoperability, and vendor-specific SLA terms must be addressed to ensure consistent quality of service and avoid vendor lock-in.

EPA will evaluate existing service level metrics across existing contracts to identify standard requirements that have evolved organically and incorporate them into guidance related to cloud statements of work, including security requirements already established. EPA will develop guidance, including standardized clauses to be incorporated into all cloud statements of work and recommended language that may be tailored to specific cloud providers. This guidance will incorporate federal cloud acquisition best practices, including roles and responsibilities, performance measures, and associated consequences for non-compliance.

EPA is interested in collaborating with other agencies that have established guidance associated with standardized cloud contract language that fully addresses OMB's requirements. Potential collaboration partners include the U.S. Department of Interior and the National Aeronautics and Space Administration.

Thank you for the opportunity to review the report. If you have any questions regarding this response, please contact Afreeka Wilson, Audit Follow-up Coordinator, of the Office of Resources and Business Operations, (202) 564-0867 or [wilson.afreeka@epa.gov](mailto:wilson.afreeka@epa.gov).

Sincerely,

VAUGHN  
NOGA

Digitally signed by  
VAUGHN NOGA  
Date: 2024.07.08  
10:41:04 -0400

Vaughn Noga  
Chief Information Officer

cc: Eric Winter  
Valerie Hopkins  
David Alvarado  
Austin Henderson  
Erin Collard  
Tiffany McNeill  
Hitch Peabody  
Pritchett Dave  
DeShelia Hall  
David Updike  
Niki Maslin  
Chi Tran  
Jennie Campbell  
Dwane Young  
Pamela Legare  
JoanB Rogers  
Celia Vaughn  
Rodney-Daryl Jones  
Yulia Kalikhman  
Gregory Scott  
Janice Jablonski  
Marilyn Armstrong  
Afreeka Wilson  
Darryl Perez  
OMS Audit Coordination  
Stuart Miles-McLean  
Kristien Knapp  
EPA GAO Liaison Team  
Susan Perkins  
EPA GAO Liaison Team

# Appendix X: Comments from the General Services Administration

DocuSign Envelope ID: 92F2A560-6CB7-4BC8-AF54-662729ED2D23



The Administrator

July 18, 2024

The Honorable Gene L. Dodaro  
Comptroller General of the United States  
U.S. Government Accountability Office  
Washington, DC 20540

Dear Comptroller General Dodaro:

The U.S. General Services Administration (GSA) appreciates the opportunity to review and comment on the U.S. Government Accountability Office (GAO) draft report, *CLOUD COMPUTING: Agencies Need to Address Key OMB Procurement Requirements* (GAO-24-106137).

GAO made the following recommendations to GSA:

- (1) The Administrator of GSA should ensure that the CIO of GSA updates guidance to put a cloud SLA in place with every vendor when a cloud solution is deployed. The guidance should include language that addresses OMB's required elements for SLAs, including: remediation plans for non-compliance. (Recommendation 36)
- (2) The Administrator of GSA should ensure that the CIO of GSA develops guidance regarding standardizing cloud SLAs. (Recommendation 37)

GSA agrees with the recommendations and will develop a plan to address them.

If you have any questions or concerns, please contact me or Kusai Merchant, Acting Associate Administrator, Office of Congressional and Intergovernmental Affairs, at (202)-501-0563.

Sincerely,

A handwritten signature in blue ink that reads "Robin Carnahan".

Robin Carnahan  
Administrator

U.S. General Services Administration  
1800 F Street NW  
Washington DC 20405-0002  
[www.gsa.gov](http://www.gsa.gov)

# Appendix XI: Comments from the National Science Foundation



U.S. National Science Foundation  
Office of the Director

July 19, 2024

Carol C. Harris  
Director, Information Technology Acquisition Management Issues  
U.S. Government Accountability Office  
441 G Street NW  
Washington, DC 20226

Dear Ms. Harris:

Thank you for the opportunity to review and provide comments on the Government Accountability Office (GAO) draft report, *Cloud Computing: Agencies Need to Address Key OMB Procurement Requirements* (GAO-24-106137). The U.S. National Science Foundation (NSF) values the GAO staff's professionalism and many constructive interactions during this GAO engagement.

NSF appreciates GAO's acknowledgement of agency efforts to establish policies and guidance related to the procurement and use of cloud computing services. As the Foundation continues to expand its use of cloud computing services, we are working to further formalize and strengthen guidance for cloud acquisitions to include standardized service level agreements (SLAs) and high value asset contract language.

NSF concurs with the recommendations made by GAO for additional actions the agency should take to establish and standardize cloud contract SLAs and to ensure contracts for high value assets reference continuous monitoring requirements.

Again, thank you for the opportunity to review and comment on this draft report. The NSF Chief Information Officer (CIO) will prepare a Corrective Action Plan (CAP) as appropriate. Please feel free to contact Veronica Shelley at [vshelley@nsf.gov](mailto:vshelley@nsf.gov) or 703-292-4384 if you have any questions or require additional information. We look forward to working with you again in the future.

Sincerely,

A handwritten signature in blue ink, appearing to read 'Sethuraman Panchanathan'.

Sethuraman Panchanathan  
Director

2415 Eisenhower Avenue, Suite 19100 | Alexandria, VA 22314



# Appendix XII: Comments from the Nuclear Regulatory Commission



UNITED STATES  
NUCLEAR REGULATORY COMMISSION  
WASHINGTON, D.C. 20555-0001

July 9, 2024


Carol C. Harris, Director  
Information Technology  
U.S. Government Accountability Office  
441 G Street, NW  
Washington, D.C. 20548

Dear Ms. Harris:

Thank you for providing the U.S. Nuclear Regulatory Commission (NRC) with the opportunity to review and comment on the U.S. Government Accountability Office's (GAO's) draft report GAO-24-106137, "Cloud Computing: Agencies Need to Address Key OMB Procurement Requirements." The NRC has reviewed the draft report, is in general agreement with the findings in the report and has a few minor comments for GAO consideration. Please see the comments in the enclosure to this letter.

If you have any questions regarding the NRC's response, please contact John Jolicoeur. Mr. Jolicoeur can be reached at 301-415-1642 or via email to [John.Jolicoeur@nrc.gov](mailto:John.Jolicoeur@nrc.gov).

Sincerely,

 Signed by Furstenau, Raymond  
on 07/09/24

Raymond V. Furstenau  
Acting Executive Director  
for Operations

Enclosure:  
NRC Comments on the Draft  
GAO Report (GAO-24-106137)

SUBJECT: U.S. NUCLEAR REGULATORY COMMISSION RESPONSE LETTER TO GAO  
 DRAFT REPORT WITH RECOMMENDATIONS, GAO-24-106137 DATED: JULY 9,  
 2024.

**DISTRIBUTION: LTR-24-0147-1-OCIO, OEDO-24-00196-OCIO**

RidsEdoMailCenter Resource  
 JMartin, EDO  
 JJolicoeur, EDO  
 SFlanders, OCIO  
 KWebber, RES/DSA  
 SCochrum, OCHCO  
 BSall, OCIO/DIME

**ADAMS Accession No.: ML24179A310 (ltr), ML24179A303 (encl)**

<b>OFFICE</b>	ADM/AMD	ADM/AMD	OGC	OCIO/SDOD	OCIO/DIME
<b>NAME</b>	JDaly	NStevenson	RBaum	GHayden	BSall
<b>DATE</b>	06/27/2024	06/28/2024	07/02/2024	06/27/2024	06/27/2024
<b>OFFICE</b>	OCIO/DIME	OCIO/OD	OEDO/AO	EDO	
<b>NAME</b>	BSall	SFlanders	JMartin	RFurstenau	
<b>DATE</b>	06/27/2024	07/01/2024	07/09/24	07/09/24	

OFFICIAL RECORD COPY

**U.S. Nuclear Regulatory Commission Comments on GAO-24-106137, “Cloud Computing: Agencies Need to Address Key OMB Procurement Requirements,” Draft Report**

The U.S. Government Accountability Office (GAO) report concludes that, though the U.S. Nuclear Regulatory Commission (NRC)’s cloud program leverages industry-vetted, FED-RAMP authorized cloud providers via federal acquisition vehicles, there was a lack of evidence supporting the use of agency-developed guidance in several areas pertaining to cloud acquisitions. As a result, GAO has provided four recommendations to the Chair of the NRC. Per the request for agency comment, NRC has provided the following comments for each recommendation:

- **GAO Recommendation 42:** The Chair of NRC should ensure that the Chief Information Officer (CIO) of NRC develops guidance to put a cloud Service Level Agreement (SLA) in place with every vendor when a cloud solution is deployed. The guidance should include language that addresses the Office of Management and Budget (OMB)’s four required elements for SLAs, including: continuous awareness of the confidentiality, integrity, and availability of its assets; a detailed description of roles and responsibilities; clear performance metrics; and remediation plans for non-compliance.

**NRC Response:** The NRC accepts GAO recommendation 42 for the CIO to develop internal guidance that aligns with OMB’s guidance on cloud service SLAs. This will bring the agency’s guidance documentation up to speed with its current practices for assessing and approving cloud service SLAs in accordance with the Federal Cloud Smart strategy.

- **GAO Recommendation 43:** The Chair of NRC should ensure that the CIO of NRC develops guidance standardizing cloud SLAs.

**NRC Response:** The NRC accepts GAO recommendation 43 for the CIO to develop internal guidance that aligns with OMB’s guidance on cloud service SLAs. This will bring the agency’s guidance documentation up to speed with its current practices for assessing and approving cloud service SLAs in accordance with the Federal Cloud Smart strategy.

- **GAO Recommendation 44:** The Chair of NRC should ensure that the CIO of NRC develops guidance to require that contracts affecting the agency’s High Value Assets (HVA)s that are managed and operated in the cloud include language that provides the agency with continuous visibility of the asset.

**NRC Response:** The NRC accepts GAO recommendation 44 for the CIO to develop internal guidance that aligns with OMB’s guidance on cloud service SLAs. This will bring the agency’s guidance documentation up to speed with its current practices for assessing and approving cloud service SLAs in accordance with the Federal Cloud Smart strategy.

- **GAO Recommendation 45:** The Chair of NRC should ensure that the CIO of NRC updates its existing contracts for HVAs, managed and operated in the cloud, to meet OMB’s requirement once guidance from the CIO Council is available on language that provides the agency with continuous visibility of the asset. If modifying the existing contract is not practical, the agency should incorporate language into the contract that will meet OMB’s requirement upon option exercise or issuance of a new award.

Enclosure

---

2

**NRC Response:** The NRC accepts GAO recommendation 45. NRC agrees to include language in contracts to ensure continuous visibility of high value assets to meet OMB requirements once guidance from the CIO Council is available.

# Appendix XIII: Comments from the Office of Personnel Management



Office of the  
Chief Information  
Officer

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT  
Washington, DC 20415

July 12, 2024

Carol C. Harris  
Director, Information Technology and Cybersecurity  
U.S. Government Accountability Office  
441 G Street, NW  
Washington, DC 20548

Dear Ms. Harris:

Thank you for the opportunity to respond to the Government Accountability Office (GAO) draft report, *Cloud Computing: Agencies Need to Address Key OMB Procurement Requirements*, GAO-24-106137.

OPM's response to the recommendation is below.

**Recommendation #46:** The Director of OPM should ensure that the CIO of OPM updates guidance to put a cloud SLA in place with every vendor when a cloud solution is deployed. The guidance should include language that addresses OMB's required element for SLAs: remediation plans for non-compliance.

**Management's Response:** OPM concurs. OPM currently has a Service Level Agreement (SLA) for OPM's Enterprise Cloud Environment. To remediate the recommendation, OPM will issue a policy to provide guidance to put SLAs in place with every vendor that deploys a cloud environment or solution. The guidance will address OMB's required SLA element (i.e., remediation plans for non-compliance).

I appreciate the opportunity to respond to this draft report. If you have any questions regarding our response, please contact Mark Lambert ((202) 606-2980, mark.lambert@opm.gov).

Sincerely,

Guy Cavallo

Digitally signed by Guy  
Cavallo  
Date: 2024.07.26  
13:45:26 -04'00'

Chief Information Officer  
U.S. Office of Personnel Management

# Appendix XIV: Comments from the Small Business Administration



U.S. SMALL BUSINESS ADMINISTRATION  
WASHINGTON, DC 20416

July 19, 2024

Daniel Garcia-Diaz  
Managing Director  
Financial Markets and Community Investment  
U.S. Government Accountability Office

Dear Mr. Garcia-Diaz:

Thank you for providing the U.S. Small Business Administration (SBA) with the opportunity to comment on the Government Accountability Office (GAO) draft report titled, "Agencies Need to Address Key OMB Procurement Requirements" (24-106137).

OCIO continues to make progress building a strong IT governance framework that will enable the agency to achieve its mission goals and objectives, as well as improve cloud policy, procurement, modernization, and Service Level Agreements (SLAs). Through an extensive revision of its cloud policies and processes, cloud systems will integrate under a unified IT governance framework to address essential improvements. The framework is still in development, but when operational, cloud acquisitions, policies, and investments will be systematically reviewed for iterative improvement, requirements, and SLAs for all Federal acquisition and security policies.

We anticipate remediation of the below recommendations by January 31, 2025.

**Recommendation 47** – The Administrator of SBA should ensure that the CIO of SBA develops guidance that requires a periodic review of the agency's policies related to cloud services, including any technical guidance and business requirements, to determine if improvements should be made.

**SBA Response:** SBA agrees with this recommendation and will ensure that SBA develops guidance that requires a periodic review of the agency's policies related to cloud services, including any technical guidance and business requirements, to determine if improvements should be made.

---

**Recommendation 48** – The Administrator of SBA should ensure that the CIO of SBA develops guidance to put a cloud SLA in place with every vendor when a cloud solution is deployed. The guidance should include language that addresses OMB’s four required elements for SLAs, including: continuous awareness of the confidentiality, integrity, and availability of its assets; a detailed description of roles and responsibilities; clear performance metrics; and remediation plans for non-compliance.

**SBA Response:** SBA agrees with this recommendation and will develop guidance to put a cloud SLA in place with every vendor when a cloud solution is deployed.

**Recommendation 49** The Administrator of SBA should ensure that the CIO of SBA develops guidance regarding standardizing cloud SLAs.

**SBA Response:** SBA agrees with this recommendation and will develop guidance regarding standardizing cloud SLAs.

Sincerely,

**STEPHEN KUCHARSKI** Digitally signed by STEPHEN KUCHARSKI  
Date: 2024.07.23 11:55:12 -04'00'

**Stephen Kucharski**  
Chief Information Officer (Acting)  
Office of the Chief Information Officer  
U.S. Small Business Administration

---

# Appendix XV: Comments from the Social Security Administration

---



**SOCIAL SECURITY**  
Office of the Commissioner

July 18, 2024

Carol C. Harris  
Director, Information Technology and Cybersecurity  
United States Government Accountability Office  
441 G Street, NW  
Washington, DC 20548

Dear Director Harris:

Thank you for the opportunity to review the Draft Report, "CLOUD COMPUTING: Agencies Need to Address Key OMB Procurement Requirements" (GAO-24-106137). We agree with the recommendation.

Please contact me at (410) 965-2611 if I can be of further assistance. Your staff may contact Hank Amato, Director of the Audit Liaison Staff, at (407) 765-9774.

Sincerely,

A handwritten signature in blue ink, appearing to read "Dustin Brown".

Dustin Brown  
Acting Chief of Staff



# Appendix XVI: Comments from the U.S. Agency for International Development



Ms. Carol C. Harris  
Director  
Information Technology Acquisition Management Issues  
U.S. Government Accountability Office  
441 G Street, N.W.  
Washington, D.C. 20226

July 15, 2024

**Re: *Cloud Computing: Agencies Need to Address Key OMB Procurement Requirements (GAO-24-106137)***

Dear Ms. Harris:

I am pleased to provide the response of the U.S. Agency for International Development (USAID) to the draft report produced by the U.S. Government Accountability Office (GAO) titled, *Cloud Computing: Agencies Need to Address Key OMB Procurement Requirements (GAO-24-106137)*. The report contains two recommendations for action on behalf of USAID.

As noted in the draft report, USAID has policies and practices in place to ensure that Service Level Agreements (SLAs) are included in all acquisitions. USAID recognizes that our existing policies do not specifically address the elements recommended for the procurement of cloud computing and will take action to update our policies to address this shortcoming.

I am transmitting this letter and the enclosed comments from USAID for inclusion in the GAO's final report. Thank you for the opportunity to respond to the draft report and for the courtesies extended by your staff while conducting this engagement. We appreciate the opportunity to participate in the complete and thorough evaluation of our Cloud Computing Procurement Management.

Sincerely,

*Colleen Allen*

Colleen Allen  
Assistant Administrator  
Bureau for Management

Enclosure: a/s

---

**COMMENTS BY THE U.S. AGENCY FOR INTERNATIONAL DEVELOPMENT ON THE DRAFT REPORT PRODUCED BY THE U.S. GOVERNMENT ACCOUNTABILITY OFFICE (GAO) TITLED, *Cloud Computing: Agencies Need to Address Key OMB Procurement Requirements* (GAO-24-106137)**

The U.S. Agency for International Development (USAID) would like to thank the U.S. Government Accountability Office (GAO) for the opportunity to respond to this draft report. We appreciate the extensive work of the GAO engagement team, and the specific findings that will help USAID achieve greater effectiveness in our Cloud Computing Procurement Management.

**The draft report contains two recommendations for USAID:**

**Recommendation 1:** The Administrator of USAID should ensure that the CIO of USAID updates guidance to put a cloud SLA in place with every vendor when a cloud solution is deployed. The guidance should include language that addresses OMB's required elements for SLAs, including: remediation plans for non-compliance.

**Recommendation 2:** The Administrator of USAID should ensure that the CIO of USAID develops guidance regarding standardized Cloud SLAs.

**USAID Response:** USAID concurs with both recommendations. The Agency is committed to addressing the key procurement requirements established by the Office of Management and Budgets (OMB) in its 2019 Cloud Smart Strategy. USAID establishes policies in its Automated Directive System (ADS). ADS Chapter 509 establishes the operational policy for the management and oversight of information-technology (IT) resources at USAID while other Agency policies, including ADS 300, ADS 302, Acquisition and Assistance Policy Directive (AAPD) 16-02 (Revised) dictate policies related to the Acquisition of Information Technology. The relevant ADS chapters will be updated to include a requirement for a Cloud Service Level Agreement (SLA) when a cloud solution is deployed. Further, the CIO will develop guidance regarding standardizing Cloud SLAs.

---

# Appendix XVII: GAO Contact and Staff Acknowledgments

---

## GAO Contact

Carol C. Harris, (202) 512-4456, or [HarrisCC@gao.gov](mailto:HarrisCC@gao.gov)

---

## Staff Acknowledgments

In addition to the individual named above, the following staff made key contributions to this report: Eric Winter (Assistant Director), Valerie Hopkins (Analyst in Charge), Joseph Andrews, Brandon Berney, Leland Buggie, Quade Bywater, Donna Epler, Rebecca Eyler, Matthew Gray, Igor Koshelev, Philip Menchaca, Brandon Mitchell, Sejal Sheth, and Haley Weller.

---

---

## GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

---

## Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its [website](#) newly released reports, testimony, and correspondence. You can also [subscribe](#) to GAO's email updates to receive notification of newly posted products.

---

## Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, <https://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

---

## Connect with GAO

Connect with GAO on [Facebook](#), [Flickr](#), [Twitter](#), and [YouTube](#).  
Subscribe to our [RSS Feeds](#) or [Email Updates](#). Listen to our [Podcasts](#).  
Visit GAO on the web at <https://www.gao.gov>.

---

## To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: <https://www.gao.gov/about/what-gao-does/fraudnet>

Automated answering system: (800) 424-5454 or (202) 512-7700

---

## Congressional Relations

A. Nicole Clowers, Managing Director, [ClowersA@gao.gov](mailto:ClowersA@gao.gov), (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

---

## Public Affairs

Sarah Kaczmarek, Acting Managing Director, [KaczmarekS@gao.gov](mailto:KaczmarekS@gao.gov), (202) 512-4800, U.S. Government Accountability Office, 441 G Street NW, Room 7149 Washington, DC 20548

---

## Strategic Planning and External Liaison

Stephen J. Sanford, Managing Director, [spel@gao.gov](mailto:spel@gao.gov), (202) 512-4707  
U.S. Government Accountability Office, 441 G Street NW, Room 7814,  
Washington, DC 20548



Please Print on Recycled Paper.