United States Government Accountability Office

Report to Congressional Committees

September 2023

# CLOUD COMPUTING

# DOD Needs to Improve Tracking of Data User Fees

Accessible Version

GAO-23-106247

# GAO Highlights

Highlights of GAO-23-106247, a report to congressional committees

## Why GAO Did This Study

Cloud computing enables agencies to have on-demand access to shared computing resources. The costs of doing so are often lower than if the agencies were maintaining the resources. In fiscal year 2022, major federal agencies obligated about $7 billion for cloud computing contracts, including approximately $3 billion by DOD. Cloud service providers charge users fees for transferring data out of the cloud—known as data egress fees. Committee reports from the Senate and House Armed Services Committees accompanying the James M. Inhofe National Defense Authorization Act for Fiscal Year 2023 include provisions for GAO to review cloud data egress fees at DOD, including their effects on vendor lock-in.

This report determines the extent to which DOD (1) considered data egress fees when procuring and implementing cloud services and their potential for vendor lock-in and (2) mitigated the impact of data egress fees and tracked and reported on them. To assess DOD's cloud data egress fees, GAO analyzed relevant department guidance on cloud services and the tracking and reporting of cloud expenditures. It also reviewed supporting department documentation on cost reporting and tracking. In addition, GAO interviewed DOD officials.

## What GAO Recommends

GAO is making one recommendation to the Department of Defense to develop a plan and time frame for adopting a tool to track data egress fees across the department. DOD concurred with the recommendation.

View GAO-23-106247. For more information, contact David B. Hinchman at (214) 777-5719 or hinchmand@gao.gov.

September 2023

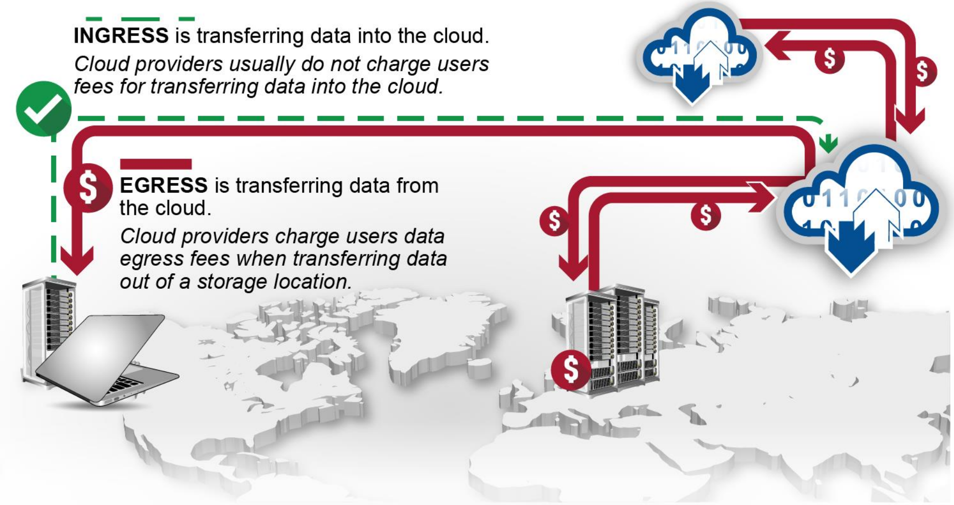
# CLOUD COMPUTING

## DOD Needs to Improve Tracking of Data User Fees

## What GAO Found

Data user fees (ingress and egress) are related to how users transfer and access data in a cloud environment. Data ingress is transferring data into the cloud and data egress is transferring data from the cloud. While data ingress is often free to users, cloud service providers generally charge data egress fees for transferring data out of storage (see figure).

**Figure: Transfer of Data into and out of the Cloud**


**INGRESS** is transferring data into the cloud.
*Cloud providers usually do not charge users fees for transferring data into the cloud.*
**EGRESS** is transferring data from the cloud.
*Cloud providers charge users data egress fees when transferring data out of a storage location.*
$

Sources: GAO analysis of market data; GAO (icons); pyty/stock.adobe.com (map). | GAO-23-106247

The Department of Defense (DOD) has begun to consider data egress fees when procuring and implementing cloud services. The department's recent contract negotiations with commercial providers resulted in discounts on data fees, including data egress fees. Vendor lock-in can happen in cloud computing when the cost of moving to a new provider is so high that a user stays with their incumbent provider. However, DOD officials stated that egress fees had not been a primary cause for vendor lock-in. These officials added that other factors could cause vendor lock-ins, including a lack of specific skills by government staff, or the reliance on cloud services unique to a specific cloud provider.

DOD has mechanisms that could mitigate the impact data egress fees could have on DOD as it procures and implements cloud services across the department. DOD officials reported that data egress fees account for less than 1 percent of known cloud expenditures. However, the department does not have the capability to track and report on these fees. In addition, DOD's contract-specific tools do not track cloud expenditures, including data egress fees department-wide. DOD officials identified improved insight into cloud expenditures through recent department-wide contracts such as the Joint Warfighting Cloud Capability—a cloud contract with four commercial service providers—and other tools. However, DOD does not yet have a plan or time frame for adopting a tool that tracks data egress fees. Until DOD acquires and implements such a tool, it will continue to lack full insight into the impact of egress fees.

# Contents

Tables

Figures

## Abbreviations

| | |
|---|---|
| ATAT | Account Tracking and Automation Tool |
| CAMO | Cloud Account Management Optimization |
| CFO Act | Chief Financial Officers Act of 1990 |
| CIO | Chief Information Officer |
| CSP | Cloud Service Provider |
| DISA | Defense Information Systems Agency |
| DOD | Department of Defense |
| GSA | General Services Administration |
| IT | Information Technology |
| JWCC | Joint Warfighting Cloud Capability |
| NIST | National Institute of Standards and Technology |
| OMB | Office of Management and Budget |
| TBM | Technology Business Management |

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.

GAO U.S. GOVERNMENT ACCOUNTABILITY OFFICE

441 G St. N.W.
Washington, DC 20548

September 12, 2023

Congressional Committees

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 option when feasible.[1] According to the National Institute of Standards and Technology (NIST), cloud computing is a means for enabling on-demand access to shared pools of configurable computing resources such as networks, servers, storage applications, and services that can be rapidly provisioned and released.[2]

In recent years, federal agencies have started to migrate their data and applications to the cloud for increased reliability, processing, and storage. In fiscal year 2022, major federal agencies[3] obligated about $7 billion on cloud computing contracts,[4] including approximately $3 billion by the Department of Defense (DOD).[5]

[1] Office of Management and Budget, *25 Point Implementation Plan to Reform Federal Information Technology Management* (Dec. 9, 2010).

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

[3] We defined major agencies as those covered by the Chief Financial Officers Act of 1990 (CFO Act). The law requires chief financial officers to oversee financial management activities at 23 civilian executive departments and agencies as well as the Department of Defense. The list of 24 entities is often referred to collectively as "CFO Act agencies." The 24 agencies are the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs; the 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, and U.S. Agency for International Development.

[4] To identify cloud computing contracts, we used a list of cloud-related product/service codes identified in General Services Administration's Federal Procurement Data System.

[5] We have ongoing work looking at the 24 CFO Act agencies' cloud procurement practices, including their use of procurement and contract data to inform decision making. We plan to issue a report in early 2024.

Cloud computing services (cloud services) offer agencies a strategy to buy services more quickly and often at a lower cost rather than building, operating, and maintaining an on-premise data center themselves. Cloud service providers (CSP) charge fees for using these services, including fees for storing, computing, and transferring data out of the cloud (data egress).[6] While data ingress (the process of transferring data into a cloud environment) is often free to users, data egress fees are user fees charged by a service provider to transfer data out of where they are stored.

The committee reports from the Senate[7] and House[8] Armed Services Committees accompanying the James M. Inhofe National Defense Authorization Act for Fiscal Year 2023[9] include provisions for GAO to conduct an assessment on data egress fees at DOD, including their effects on vendor lock-in.[10] Our objectives for this review are to determine the extent to which DOD (1) considered data egress fees when procuring and implementing cloud services and their potential for vendor lock-in and (2) mitigated the impact of data egress fees and tracked and reported on them.

For the first objective, we identified DOD guidance on considering cloud costs, including data egress fees when acquiring and using cloud services. We then compared DOD guidance with information from DOD and relevant military departments on the impact of cloud expenditures, including egress fees, on the procurement and implementation of cloud services. We also reviewed memos documenting the results of negotiations on egress fees between DOD and the CSPs on the Joint Warfighting Cloud Capability (JWCC) contract to understand how egress fees were considered as part of the JWCC contract. We interviewed federal officials regarding the impact of egress fees on vendor lock-in associated with cloud computing. These interviews included officials from federal agencies with a lead role in providing guidance for cloud computing—OMB and the General Services Administration (GSA)—as

[6] When we discuss cloud computing or cloud service providers in this report, we are referring to commercial cloud service providers.

[7] S. Rep. No. 117-130, at 316-317 (July 18, 2022).

[8] H.R. Rep. No. 117-397, at 318-319 (July 1, 2022).

[9] James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, Pub. L. No. 117-263, 136 Stat. 2395 (Dec. 23, 2022).

[10] Vendor lock-in can happen when the cost of moving to a new CSP is so high that a user stays with the incumbent provider.

well as DOD cloud computing offices. We also interviewed DOD and military department officials to verify the information collected. Additionally, we interviewed officials from three major CSPs to obtain their views on data egress fees, cost reporting and tracking tools, and vendor lock-in.

For the second objective, we assessed documentation from DOD and commercial CSPs on mechanisms used to mitigate or avoid data egress fees, including when and how these are used. We also summarized documentation from DOD, OMB, and GSA regarding guidance for the tracking and reporting of cloud expenditures. We then assessed supporting documentation, such as DOD and the Air Force Cloud One program's cost reporting data. Cloud One is the Air Force's cloud brokering service. According to the DOD Office of the Chief Information Officer (CIO) Software Modernization Plan, DOD cloud brokers are to support cloud adoption for DOD. They are to analyze current systems' environments, determine what is needed from a technical, security, and cost perspective, and understand the breadth of cloud services available to DOD users. We also compared the information with existing guidance. We interviewed DOD, military department, and CSP officials to verify the information collected. To determine the reliability of the Air Force Cloud One data, we electronically tested their calendar year 2022 expenditures, including egress fees, for errors by checking for missing data and recalculating the percentage of egress fees charged as a percentage of the overall fees paid. We determined that the data were sufficiently reliable for our purposes.[11]

We conducted this performance audit from October 2022 to September 2023 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.

## Background

Cloud computing is a means for enabling on-demand access to shared pools of configurable computing resources (e.g., networks, servers,

[11] We were unable to assess the reliability of DOD and Army's cloud egress fee data because officials told us they were estimates and they could not provide supporting documentation.

storage applications, and services) that can be rapidly provisioned. By purchasing IT services through a commercial CSP, agencies can 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.** Capabilities are available to agencies over any 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.** Capabilities can be provisioned by agencies to meet demand by scaling resources up or down, adding or removing processing or memory capacity, or both.
- **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.

## DOD Cloud Environment

DOD is a complex organization and the largest U.S. government department. In support of its military operations, the department manages many IT investments, including investments in business, communications, and command and control systems. It also spends billions of dollars annually to build and maintain these systems. DOD has also reported spending billions of dollars for cloud computing services.

Specifically, in 2022, we reported that in fiscal year 2022, DOD planned to spend approximately $38.6 billion on unclassified IT investments. Of this, the department reported to OMB that it planned to spend $1.1 billion for cloud services and migration. This included $798 million for commercial or in-house cloud services, and $329 million related to migrating systems to cloud services. According to GSA's Federal Procurement Data System, DOD obligated over $3 billion on cloud computing contracts in fiscal year 2022.[12]

DOD has several key cloud initiatives that it plans to use to help accelerate its cloud adoption. One is an enterprise-level cloud contract; others serve as cloud brokers and support DOD entities in accessing the cloud. These efforts include the following:

- **DOD's Joint Warfighting Cloud Capability (JWCC).** Operated by DOD's Defense Information Systems Agency (DISA), JWCC is intended to be an enterprise-level cloud contract. It is designed to provide DOD entities with a contract to acquire commercial cloud services directly from providers at all security levels. JWCC is an indefinite delivery/indefinite quantity[13] contract awarded in December 2022 to four commercial CSPs.[14] It has a maximum value of $9 billion. The first task orders on the contracts were issued in March 2023.
- **Army's Cloud Account Management Optimization (CAMO).** Operated by Army's Enterprise Cloud Management Agency as a brokerage for Army cloud users, CAMO is a prototype cloud initiative to consolidate Army cloud contracts under a single contract. It began the second option year of its prototype in January 2021.
- **Air Force Cloud One Contract.** Operated by Air Force's Office of the CIO as a brokerage run by a third party service, Cloud One is to support Air Force cloud applications under one contract. Air Force mission systems were directed to begin moving to Cloud One in June 2021.
- **Navy Cloud Service Management Organization.** Established in 2020, and operated by Navy's Program Executive Office Digital as a brokerage office, the organization is to implement an enterprise model for the Department of the Navy. Navy officials stated that they expect their cloud effort to reach initial operating capability in Fiscal Year 2024.

[12] We discuss our prior report on DOD's cost reporting practices, including potential underreporting in DOD's cloud spending later in the report.

[13] An indefinite delivery/indefinite quantity contract is awarded to one or more contractors when the exact quantities and timing for products or services are not known at the time of the award.

[14] The four cloud service providers that are part of the JWCC contract are Oracle Cloud Infrastructure, Google Cloud, Microsoft Azure, and Amazon Web Services.

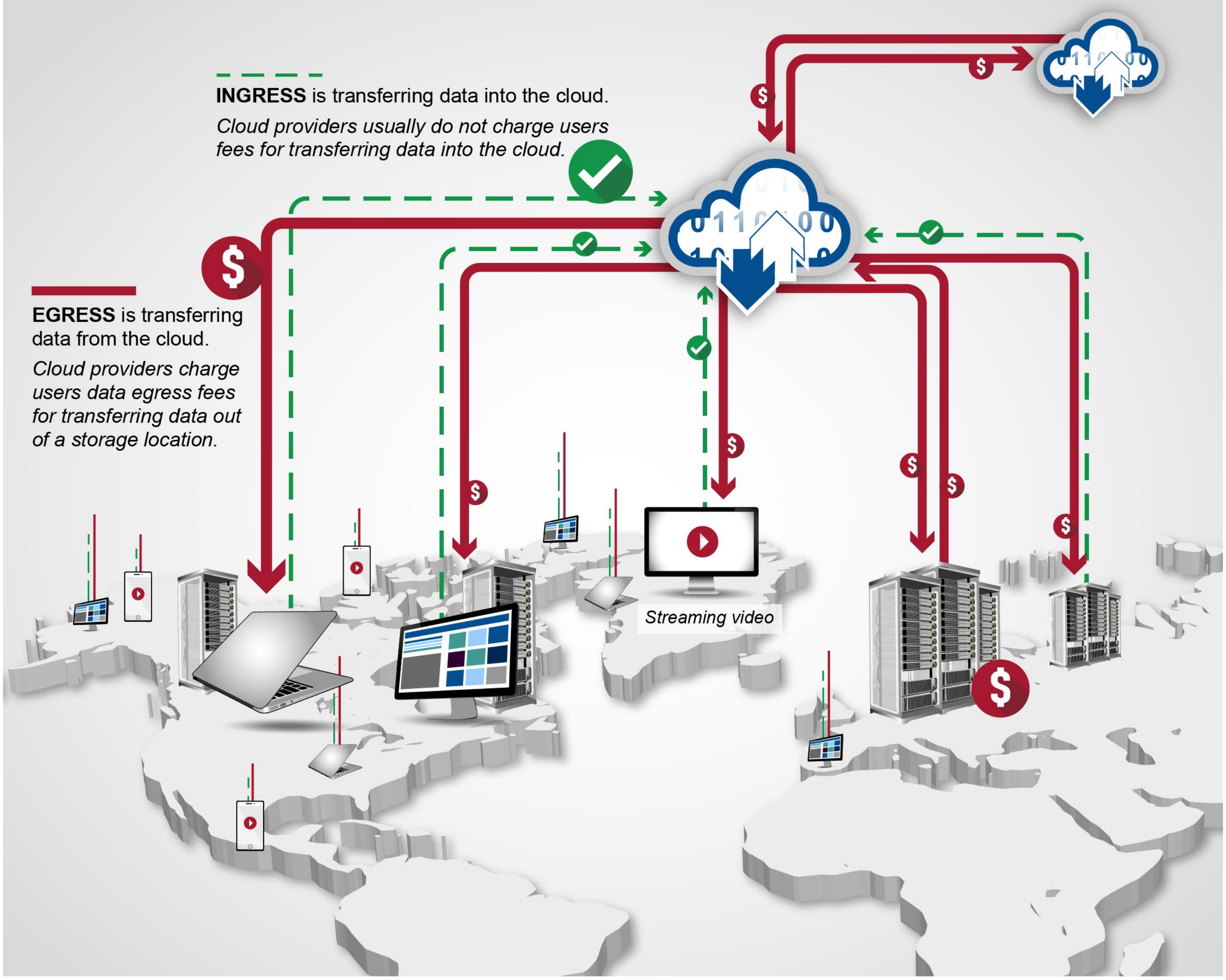
## Cloud Data User Fees

Commercial CSPs charge users fees for a wide variety of cost components, including computing capacity, storage, storage type, transactions, networks, data security, and transferring data in and out of the cloud (data ingress and egress). Two of these user fees, data ingress and egress, are related to how users transfer and access data in a cloud environment. Specifically, data ingress is the process of transferring data into a cloud environment. Conversely, egress occurs when users transfer and access data from a storage location to enable data to be used or processed in some way—for example, an individual streaming cloud-stored video on a desktop or mobile device, or an analyst pulling financial data stored in the cloud to local storage. While data ingress is often free to users, service providers generally charge data egress fees for transferring data out of a storage location. Examples of data egress that could incur charges include moving data

- between cloud instances from the same provider in different regions or availability zones;
- from the cloud to individual users (such as with downloading data to a local desktop);
- from the cloud to an on-premise data center; or
- from one security level to another (such as from unclassified to the secret classification level).

Egress also occurs when transferring data from one vendor to another, such as at the end of a contract. See figure 1 below for a more detailed depiction of where cloud data ingress and egress occurs.

Figure 1: Transfer of Data to and from the Cloud


INGRESS is transferring data into the cloud.
Cloud providers usually do not charge users fees for transferring data into the cloud.
EGRESS is transferring data from the cloud.
Cloud providers charge users data egress fees for transferring data out of a storage location.
Streaming video
$

Sources: GAO analysis of market data; GAO (icons); pyty/stock.adobe.com (map). | GAO-23-106247

Pricing for egress is calculated on a per gigabyte basis. See table 1 for an example of data egress pricing from one CSP.

**Table 1: Sample Pricing for Commercial Egress from One Cloud Service Provider as of February 2023**

| Data transfer | Price per gigabyte |
|---|---|
| Ingress[a] | $0.00 |
| Data transfer between Availability Zones[b] (Ingress and Egress[c]) | $0.01 |
| Within same Availability Zone | $0.00 |
| Between regions within North America | $0.02 |
| Between regions within Europe | $0.02 |
| Between regions within Asia | $0.08 |
| Between regions within Oceania | $0.08 |
| Between regions within Middle East and Africa | $0.08 |
| Between regions within South America | $0.16 |

Source: Microsoft Azure Pricing Website accessed February 2, 2023 | GAO-23-106247

[a] Ingress is the action of transferring data into the cloud.

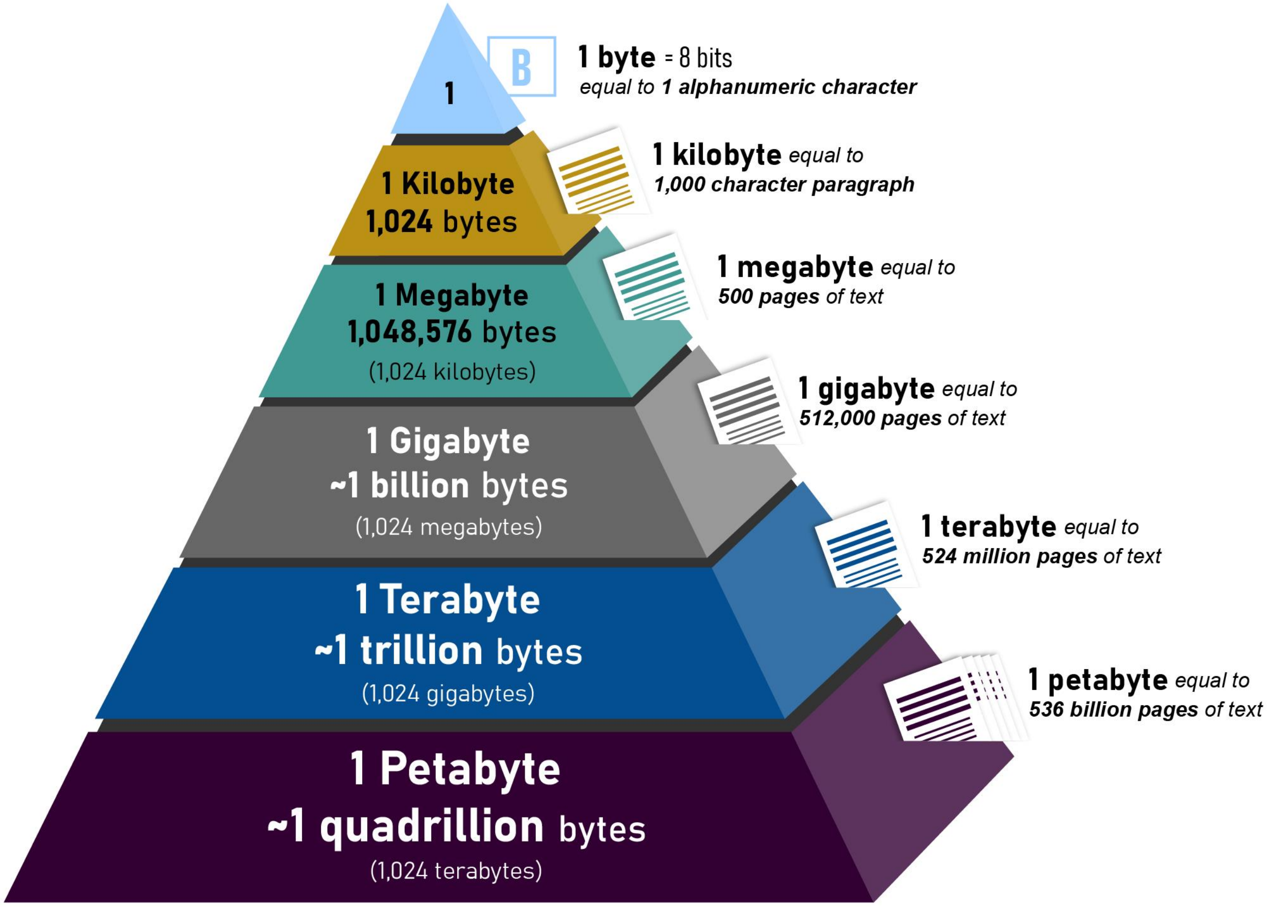
[b] An availability zone is a cloud service provider's data center that contains its own power source, network, and cooling.

[c] Egress is the action of transferring the data outside the cloud.

To provide context for the scope and scale of the volume of data in a cloud system, 1 gigabyte of data could contain 512,000 pages of text while 1 petabyte of data could contain 536 billion pages of text.[15] Figure 2 shows an example of data volume.

[15] As context, the 2022 version of the Merriam-Webster Dictionary is 960 pages long. See Merriam-Webster, *Merriam-Webster's Collegiate Dictionary* (Springfield, MA: 2022).

Figure 2: Sample Depiction of Approximate Data Volume



Source: GAO images and data analysis. | GAO-23-106247

## Prior GAO Reports on DOD Cloud and IT Cost Tracking and Reporting

We have previously reported on DOD's use of cloud services, including cloud service spending. For example, in April 2019, we found that while OMB required agencies to report on cost savings from moving to the cloud, DOD had not tracked or reported on cost savings associated with its migration to cloud services.[16] We recommended that the Secretary of

[16] GAO, *Cloud Computing: Agencies Have Increased Usage and Realized Benefits, but Cost and Savings Data Need to Be Better Tracked,* GAO-19-58 (Apr. 4, 2019).

Defense ensure that DOD's Chief Information Officer established a consistent and repeatable mechanism to track savings and cost avoidances from the migration and deployment of cloud services. DOD did not concur with this recommendation. Specifically, DOD stated that it did not agree with our recommendation because there was no standard, consistent way to capture such savings or cost avoidance. The department stated that it would work with OMB on whether or how to collect such information, and, if practical, report such information in accordance with OMB guidance.

As of October 2022, an official from DOD's Office of the Chief Information Officer reported that DOD did not intend to take action to address the recommendation. However, we continue to believe that tracking savings and cost avoidances for cloud initiatives is necessary to ensure that DOD is effectively managing and overseeing its cloud initiatives. Additionally, this would enable OMB and Congress to have sufficient data to see the results of these initiatives and understand whether DOD is achieving savings using cloud services.

Further, in June 2022 we found that, due to shortcomings in DOD's cost reporting and Technology Business Management (TBM) [17] practices, DOD was likely underreporting the total amount spent on cloud.[18] We recommended, among other things, that DOD update department-wide guidance regarding TBM implementation to include more specific information, including how the department should allocate spending for cloud services to specific cost categories. DOD did not concur with our recommendation. The department noted that the CIO issues guidance based on and in compliance with OMB policy, including TBM implementation. The department stated that components are responsible for data quality and the DOD CIO relies on their quality control to ensure data quality. Further, DOD stated that component CIOs and chief financial officers are required to submit a memorandum to the DOD CIO stating that their electronic budget submission is complete and accurate.

However, based on the issues that we identified with the completeness of DOD's cloud spending data, the DOD CIO's reliance on components' quality control processes is not sufficient to ensure quality TBM data.

[17] Technology Business Management is an IT management framework that implements a standard way to categorize IT costs, technologies, resources, applications, and services in order to disaggregate IT spending into consistent categories to provide Chief Information Officers with a detailed understanding of their organization's IT costs. These categories include the finance, IT, and business views.

[18] GAO, *Cloud Computing: DOD Needs to Improve Workforce Planning and Software Application Modernization,* GAO-22-104070 (June 29, 2022).

Accordingly, ensuring that components understand how they are supposed to allocate TBM spending, and the control processes necessary for quality data, is critical to assuring that the department's TBM investment data is reliable. Consequently, we believe our recommendation to the department to update its guidance in these areas is still warranted.

## DOD Has Begun to Consider Data Egress Fees in Procuring Cloud Services

According to DOD's Requirements for the Acquisition of Digital Capabilities Guidebook, costs must be considered prior to pursuing cloud services, including data egress fees.[19] Additionally, in 2011, OMB required agencies to implement cloud services whenever there was a secure, reliable, and cost-effective option to do so.[20] OMB further reiterated this requirement in its 2019 Federal Cloud Computing strategy.[21]

In establishing its recent enterprise-wide cloud contract, DOD considered data egress fees when procuring and implementing cloud services. Specifically, DOD's recent JWCC contract negotiation with commercial CSPs resulted in discounts on various fees better than those available commercially. The negotiations resulted in significant discounts on egress fees ranging from 35 percent to 100 percent. According to the JWCC program manager, negotiated baseline discounts in the JWCC contract provide a starting point for mission owners to negotiate for further discounts on task orders based on their needs. The program manager noted that the mission owner would then issue a task order dependent upon several factors, such as the best technical capabilities, or best (overall) value. The manager further noted that decisions are based on specific mission needs and that egress fees could play a minor role in their decision-making.

Furthermore, DOD considered egress fees for the JWCC contract and DOD CIO and military department officials separately noted that they

[19] Office of the Department of Defense Chief Information Officer, *Requirements for the Acquisition of Digital Capabilities Guidebook* (February 2022).

[20] Office of Management and Budget, *Federal Cloud Computing Strategy* (Washington, D.C.: Feb. 8, 2011).

[21] Office of Management and Budget*, Federal Cloud Computing Strategy* (Washington, D.C.: June 24, 2019).

consider data egress fees as part of the cost of other cloud programs. The officials noted that egress fees were not a driving factor in their decision-making when selecting and implementing cloud options. Rather, they stated that their cloud acquisitions focused on addressing technical considerations and that cost was not the primary consideration of moving to the cloud. DOD CIO officials further stated that in making business investment decisions regarding moving to the cloud, hosting costs are only a small portion of overall project costs. Moreover, specific cloud charges, such as egress fees, are an even smaller portion of total project costs.

## Data Egress Fees Were Not Identified as a Primary Cause of Vendor Lock-in

A recent House report described vendor lock-in as a situation when the costs of switching vendors “are sufficiently high that users stay with an incumbent firm rather than switch to a firm whose product or service they would prefer.”[22] According to various officials and cloud service providers, data egress was not identified as a cause for vendor lock-in. Rather, they noted that other factors, such as unique cloud service offerings or skill set, could result in vendor lock-in.

Specifically, DOD, GSA, and OMB officials stated that they have not heard of egress fees being a cause of vendor lock-in with CSPs from federal agencies. GSA officials and OMB officials from the Office of Federal Procurement Policy and the Office of the Federal Chief Information Officer noted that they were not aware of any issues associated with egress fees, including vendor lock-in. GSA officials noted that egress fees are program- and project- specific and that information about fees is defined in the task order.

According to DOD Office of the CIO, Air Force, and Army officials, vendor lock-in could be a consideration for any technology choice. The officials noted that with cloud computing, critical factors tend to be a lack of specific government staff skills to manage the application, or a reliance on specific cloud services that are unique to a particular cloud provider. Army officials also noted, while egress fees were not a primary cause of vendor lock-in, they noted that migrating data and systems from one service provider to another could be a large financial burden due to the amount of

[22] U.S. House Committee on the Judiciary; *Investigation Of Competition In Digital Markets,* H. Prt. 117-8, part I, at 31-32 (Washington, D.C.: Government Publishing Office, 2022.)

time and work needed. Officials from one CSP also identified this as a potential issue.

## DOD Has Mitigated Some Egress Fees, but Fee Tracking Is Limited

DOD's Acquisition of Digital Capabilities Guidebook states that program managers should regularly monitor and report metrics to ensure cloud services meet requirements as expected.[23] Further, according to the guidebook requirements, a business case analysis or similar analysis should facilitate comparison of alternatives and define expected costs, benefits, operational impacts, and risk. In addition, in its fiscal year 2019 guidance, OMB began requiring agencies to report spending on IT investments, including IT investments that leverage cloud services, using the TBM framework.[24]

DOD has mechanisms that may reduce the impact data egress fees could have on the department as cloud services are procured and implemented across the department. Specifically, DOD identified some actions to reduce or mitigate potential data egress fees as part of its efforts to plan for and implement cloud computing:

- **Physical data transfer.** The use of physical data transfer mechanisms, for example, mobile computing in the form of a semi-trailer load of computing power to physically transfer data to, from, and within the cloud may allow the department to avoid some egress fees.
- **Direct network connections.** The use of data transfers, such as direct network connections, between DOD private networks and commercial CSPs, which avoids the internet, may help avoid some fees, including egress fees.
- **Edge computing.** The use of "edge" computing that would process data locally and only move and store the results in the cloud could reduce overall egress fees.

[23] Office of the Department of Defense Chief Information Officer, *Acquisition of Digital Capabilities Guidebook* (February 2022).

[24] Office of Management and Budget, *FY 2019 IT Budget–Capital Planning Guidance* (Aug. 1, 2017).

- **Negotiated reduced egress fees.** The use of negotiated better-than-commercially-available rates for data egress fees has, in some cases, resulted in a 100 percent discount on fees.

In calendar year 2022, the Air Force Cloud One program spent around 1 percent of total cloud fees on egress fees. Additionally, DOD Office of the CIO, Army, and Navy officials stated that data egress fees currently have a minimal impact on the department's implementation of cloud services and have generally been under 1 percent of total measurable fees for cloud services that they are able to track. However, DOD does not have the capability to track and report on data egress fees across the department.

DOD and the military department CIO offices use various tracking and reporting tools for cloud expenditures. However, the tools are specific to the contracts and are not able to track data egress fees across the department. For example, the JWCC tool does not break out cloud expenditures in enough detail to include data egress fees, and the Army tool provides only an estimate of egress fee charges (see table 2).

**Table 2: Department of Defense (DOD) Tools and Methods for Tracking and Reporting Cloud Expenditures, Including Egress Fees, as of May 2023**

| Agency or department | Tool | Tool scope (applicable contract) | Description | Identified limitations |
|---|---|---|---|---|
| Department of Defense—Defense Information Systems Agency (DISA)[a] | Account Tracking and Automation Tool (ATAT) | Joint Warfighting Cloud Capability (JWCC) | JWCC's ATAT tool is a cloud provisioning and financial reporting tool that completes the initial provisioning of accounts across multiple cloud vendors at all classification levels. The tool provides financial reporting features at the task order and enterprise level to help DOD understand the usage of cloud services. | A DISA official stated that cloud expenditures are not broken out in enough detail to identify egress fees. |

| Agency or department | Tool | Tool scope (applicable contract) | Description | Identified limitations |
|---|---|---|---|---|
| Army—Enterprise Cloud Management Agency | CloudTracker | Cloud Account Management Optimization (CAMO) | The CloudTracker tool consolidates the amount spent on each cloud service provider into one dashboard and separates product and usage costs in near-real time. This is intended to allow users to identify the total operating cost of each cloud product on an hourly basis, including the amount of the egress fee. Further, this tool has allowed Army to use financial operations rather than capital expenditure models.[b] | Army officials stated that the egress fees listed in CloudTracker is a best guess estimate. Army officials explained that this is due to the different labelling of egress fees from the provider's cost reporting tools. |
| Air Force—Office of the Chief Information Officer | Cloud One Portal | Cloud One Contract | The Cloud One Portal tool enables the tracking and reporting of cloud expenditures including data egress on a project-by-project basis. | Air Force officials stated that instead of near-real time analysis, this tool tracks and reports cloud expenditures including data egress fees on a monthly basis. In addition, Air Force officials stated that they do not have insight into the data. They added that this is because a third party presents them as an overall cost, including the third party's overhead expenses, rather than breaking out individual costs. |
| Navy—Program Executive Office Digital | Cloud Control Tower | Navy Cloud Service Management Organization | The Cloud Control Tower tool is intended to provide insight into Navy's cloud expenditures, including egress. | Navy officials stated that this tool is currently in testing and is planned for use by the end of September 2023. However, the tool will be limited to reporting only on the cloud expenditures that are under the Navy Cloud Service Management Organization. |

Source: GAO Analysis of DOD Data. | GAO-23-106247

[a] DISA provides network operations, command, control, information-sharing capabilities and a global information infrastructure to support DOD.

[b] A financial operations expenditure model is when an organization manages expenditures on a real-time basis (such as by purchasing a service on a monthly basis) while a capital expenditure model involves purchasing fixed assets for a particular cycle of time (for example, developing and operating a data center for a decade).

DOD OCIO officials stated that they are not able to track egress fees because of a lack of department-wide contracts and tools for insight into costs and fees. In addition, agency officials noted that it is difficult to compare different types of fees, including egress fees, due to varying cost labeling of these fees across the various CSPs.

DOD OCIO officials noted that they are in the process of implementing department-wide contracts, such as JWCC, to provide better and more consistent cost and expenditure transparency across DOD.[25] The officials also noted that they are exploring tracking and reporting tools that could be used to provide visibility into data egress fees, across any commercial CSP used at DOD. However, the department has not developed a plan or time frame for adopting such a tool enterprise-wide.

Having complete data on egress fees for cloud services is important to ensure that DOD can provide effective management and oversight of their cloud use. Until such time, DOD will continue to lack insight into the impact of egress fees.

## Conclusions

DOD has recently begun to consider data egress fees when procuring and implementing cloud services and has mechanisms in place that may help mitigate the impact of the fees. These efforts have resulted in fee reduction or even avoidance of the charges altogether. However, it lacks the ability to track and report on data egress fees. DOD CIO officials noted that they are exploring tracking and reporting tools to provide visibility into data egress fees at DOD, across any cloud service provider or contract. However, without a plan and time frame for implementing such a tool, DOD cannot be assured that it fully understands how much is being spent on data egress or that the department’s investment in cloud services is being made as efficiently as possible.

## Recommendation

We are making one recommendation to DOD:

The Secretary of Defense should direct the DOD Chief Information Officer to develop a plan and time frame for adopting a tool to track and report cloud data egress fees across the department. (Recommendation 1)

[25] As noted earlier, the JWCC contracts were awarded in December 2022 and first used in late March 2023.

## Agency Comments

We provided a draft of this product to DOD for review and comment. We also provided a draft for comment to GSA and OMB. In its written comments (reprinted in appendix I), DOD concurred with, and described plans to address, our recommendation. Specifically, the department stated that by the third quarter of fiscal year 2025, it will develop a plan to expand the department's cloud financial operations to include the management of data egress fees.

A GSA official from the Office of the Chief Financial Officer, Office of Audit Management and Accountability stated via email that the agency had no comments on the draft report. OMB did not provide comments.

We are sending copies of this report to the appropriate congressional committees, the Secretary of Defense, the Director of OMB, the Administrator of GSA, and other interested parties. In addition, the report is 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 me at (214) 777-5719 or at hinchmand@gao.gov. Contact points for 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 II.

David B Hinchman

David B. Hinchman
Director, Information Technology and Cybersecurity

*List of Committees*

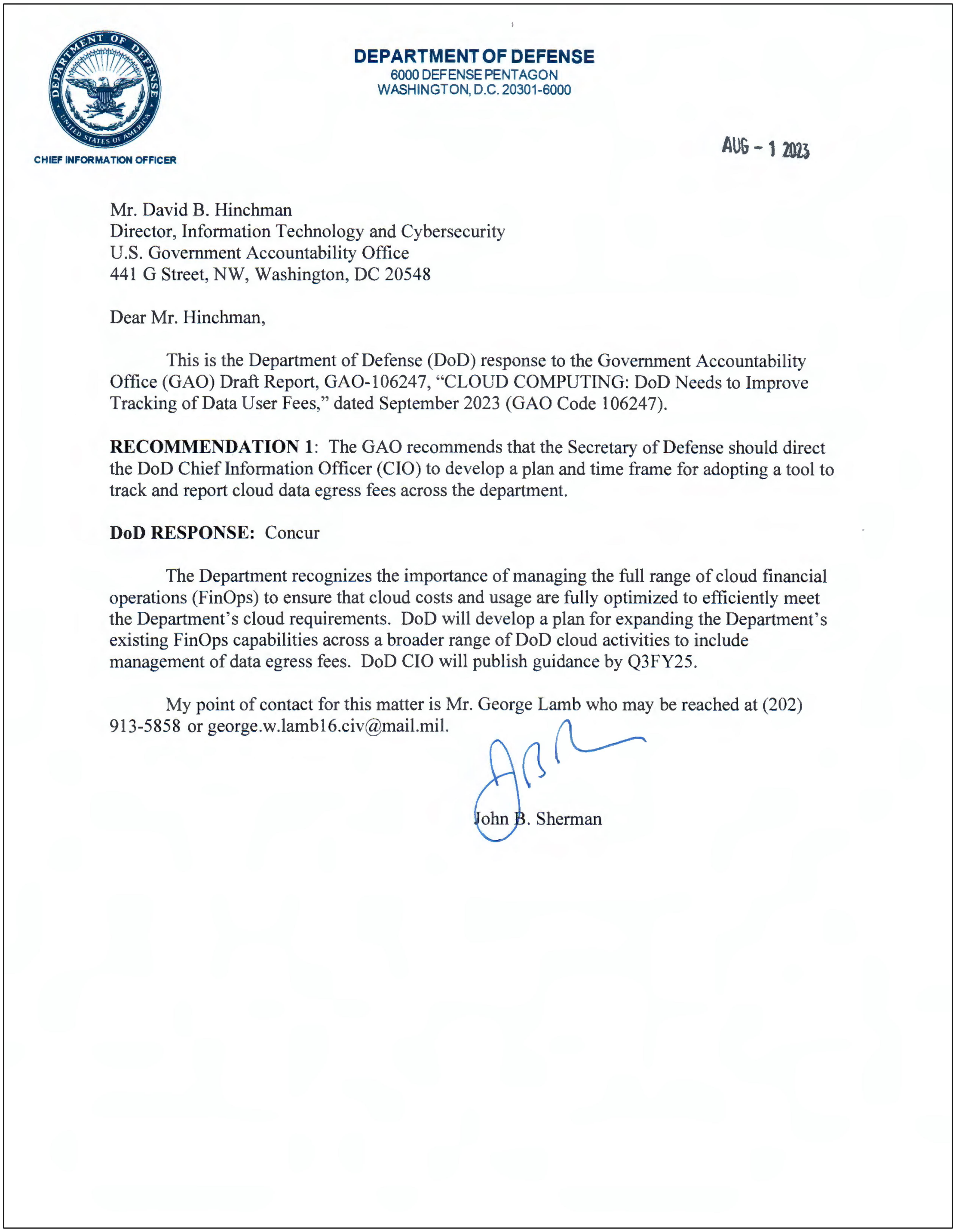
The Honorable Jack Reed
Chairman
The Honorable Roger Wicker
Ranking Member
Committee on Armed Services
United States Senate

The Honorable Jon Tester
Chair
The Honorable Susan Collins
Ranking Member
Subcommittee on Defense
Committee on Appropriations
United States Senate

The Honorable Mike Rogers
Chairman
The Honorable Adam Smith
Ranking Member
Committee on Armed Services
House of Representatives

The Honorable Ken Calvert
Chair
The Honorable Betty McCollum
Ranking Member
Subcommittee on Defense
Committee on Appropriations
House of Representatives

# Appendix I: Comments from the Department of Defense



DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

CHIEF INFORMATION OFFICER

AUG - 1 2023

Mr. David B. Hinchman
Director, Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street, NW, Washington, DC 20548

Dear Mr. Hinchman,

This is the Department of Defense (DoD) response to the Government Accountability Office (GAO) Draft Report, GAO-106247, "CLOUD COMPUTING: DoD Needs to Improve Tracking of Data User Fees," dated September 2023 (GAO Code 106247).

**RECOMMENDATION 1**: The GAO recommends that the Secretary of Defense should direct the DoD Chief Information Officer (CIO) to develop a plan and time frame for adopting a tool to track and report cloud data egress fees across the department.

**DoD RESPONSE:** Concur

The Department recognizes the importance of managing the full range of cloud financial operations (FinOps) to ensure that cloud costs and usage are fully optimized to efficiently meet the Department's cloud requirements. DoD will develop a plan for expanding the Department's existing FinOps capabilities across a broader range of DoD cloud activities to include management of data egress fees. DoD CIO will publish guidance by Q3FY25.

My point of contact for this matter is Mr. George Lamb who may be reached at (202) 913-5858 or george.w.lamb16.civ@mail.mil.

John B. Sherman

# Accessible Text for Appendix I: Comments from the Department of Defense

AUG - 1 2023

Mr. David B. Hinchman
Director, Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street, NW, Washington, DC 20548

Dear Mr. Hinchman,

This is the Department of Defense (DoD) response to the Government Accountability Office (GAO) Draft Report, GAO-106247, “CLOUD COMPUTING: DoD Needs to Improve Tracking of Data User Fees,” dated September 2023 (GAO Code 106247).

RECOMMENDATION 1: The GAO recommends that the Secretary of Defense should direct the DoD ChiefInformation Officer (CIO) to develop a plan and time frame for adopting a tool to track and report cloud data egress fees across the department.

DoD RESPONSE: Concur

The Department recognizes the importance of managing the full range of cloud financial operations (FinOps) to ensure that cloud costs and usage are fully optimized to efficiently meet the Department's cloud requirements. DoD will develop a plan for expanding the Department's existing FinOps capabilities across a broader range of DoD cloud activities to include management of data egress fees. DoD CIO will publish guidance by Q3FY25.

My point of contact for this matter is Mr. George Lamb who may be reached at (202) 913-5858 or george.w.lamb16.civ@mail.mil.

John B. Sherman

# Appendix II: GAO Contact and Staff Acknowledgments

## GAO Contact

David B. Hinchman at (214) 777-5719, hinchmand@gao.gov

## Staff Acknowledgments

In addition to the contact named above, the following staff made key contributions to this report: Neelaxi Lakhmani (Assistant Director), Kara Lovett Epperson (Analyst-in-Charge), Andrew Knox, Christopher Businsky, Lauri Barnes, and Donna Epler.

## 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, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

## Public Affairs

Chuck Young, Managing Director, youngc1@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, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548

Please Print on Recycled Paper.