United States Government Accountability Office

Report to Congressional Committees

November 2026

FEDERAL DATA CENTERS

Congress Has an Opportunity to Improve Agencies' Acquisition and Operations

GAO-27-108971

GAO Highlights

FEDERAL DATA CENTERS

Congress Has an Opportunity to Improve Agencies' Acquisition and Operations

GAO-27-108971 November 2026

A report to congressional committees

For more information, contact: Carol Harris at harriscc@gao.gov.

What GAO Found

Of the 24 Chief Financial Officers Act agencies, 21 reported having data centers. Those 21 agencies varied in incorporating the Office of Management and Budget's (OMB) five acquisition and operational requirements into the management and planning of their data centers. As of August 2026, none of the agencies had fully addressed all five requirements. For example, nine agencies reported using automated tools to monitor data center operations but the documentation they provided did not always reflect this. In addition, for the five agencies with new data centers, all of them partially addressed the requirement to incorporate energy and water usage into decision-making. Furthermore, many agencies reported meeting mission availability requirements but did not demonstrate that they had a process for managing risks to determine the maximum tolerable duration and frequency of downtime for their data centers.

Extent to Which Federal Agencies Addressed OMB's Acquisition and Operational Requirements for Data Centers, as of August 2026

Requirement	Fully addressed	Partially addressed	Not addressed
Make key data center decisions at the agency level	10	11	0
Monitor data center operations using automated tools	10	9	2
Incorporate energy and water usage into decision-making[a]	0	5	0
Meet mission availability requirements	2	19	0
Meet information security and physical security requirements	4	17	0

Legend: Fully addressed = The agency fully addressed all of the requirement's evaluation criteria. Partially addressed = The agency fully or partially addressed some, but not all, of the requirement's evaluation criteria. Not addressed = the agency did not address any of the requirement's evaluation criteria.

Source: GAO analysis of agency documentation. | GAO-27-108971

[a] The requirement was not applicable for 16 agencies because they reported having no new data centers and OMB did not require agencies to apply the requirement to existing data centers.

GAO is not making recommendations to the agencies because, in accordance with the Federal Data Center Enhancement Act (FDCEA) of 2023, the OMB requirements expired on September 30, 2026. Since the law was enacted in 2023, the IT landscape has changed. Advances in artificial intelligence capabilities and its growing use among agencies have further increased demand for high-performance computing provided by data centers. Congress has introduced various legislative proposals for data centers that are intended to, among other things, address data center energy use reporting. Although these apply more broadly to data centers nationwide, they may also impact federal data centers. If Congress takes legislative action to reauthorize or replace the FDCEA, it has the opportunity to direct OMB to update requirements for agencies to continue their efforts to enhance the cybersecurity, resiliency, and availability of data centers.

Why GAO Did This Study

Federal agencies use data centers for their mission-critical data and operations. In December 2023, Congress passed the Federal Data Center Enhancement Act of 2023 to ensure high standards of cybersecurity, resiliency, and availability for federal data centers. In response, in January 2025, OMB established five minimum requirements for acquiring and operating federal data centers. Agencies were to have satisfied these requirements by January 14, 2026, for agency-operated data centers, with potentially later dates for contractor-operated data centers.

The act includes a provision for GAO to annually review and verify the compliance of the 24 Chief Financial Officers Act agencies with OMB's requirements for new and existing data centers. In this third and final review, GAO's objective was to determine the extent to which federal agencies have incorporated OMB's acquisition and operational requirements for data centers.

GAO analyzed 21 agencies' data center documentation, including policies, procedures, and risk management and security plans. GAO then assessed the results of the analysis against the five OMB requirements. GAO also interviewed relevant agency officials.

What GAO Recommends

Congress should consider reauthorizing the FDCEA or replacing it with a new law reflecting updated priorities and OMB's acquisition and operational requirements for agencies' data centers.

Contents

Letter		1
	Background	3
	Federal Agencies Varied in Incorporating OMB's Acquisition and Operational Requirements for Their Data Centers	14
	Conclusions	21
	Matter for Congressional Consideration	22
	Agency Comments	22
Appendix I	Objective, Scope, and Methodology	24
Appendix II	Detailed Assessment of Agencies' Incorporation of OMB's Data Center Requirements	27
Appendix III	Comments from the Social Security Administration	50
Appendix IV	GAO Contact and Staff Acknowledgments	51

Tables

Table 1: Office of Management and Budget's (OMB) Five Requirements for Acquiring and Operating Federal Data Centers	10
Table 2: Agency-Reported Number of Existing and New Data Centers, as of March 2026	13
Table 3: Extent to Which Federal Agencies Incorporated the Office of Management and Budget's Five Acquisition and Operational Requirements for their Data Centers, as of August 2026	14
Table 4: Evaluation Criteria Associated with the Office of Management and Budget's (OMB) Requirements for Acquiring and Operating Federal Data Centers	25
Table 5: Extent to Which Department of Agriculture Addressed the Five Office of Management and Budget Acquisition and Operational Data Center Requirements, as of August 2026	27

Table 6: Extent to Which Department of Commerce Addressed the Five Office of Management and Budget Acquisition and Operational Data Center Requirements, as of August 2026 28
Table 7: Extent to Which Department of Defense (DOD) Addressed the Five Office of Management and Budget Acquisition and Operational Data Center Requirements, as of August 2026 29
Table 8: Extent to Which Department of Energy Addressed the Five Office of Management and Budget Acquisition and Operational Data Center Requirements, as of August 2026 31
Table 9: Extent to Which Department of Health and Human Services (HHS) Addressed the Five Office of Management and Budget Acquisition and Operational Data Center Requirements, as of August 2026 32
Table 10: Extent to Which Department of Homeland Security (DHS) Addressed the Five Office of Management and Budget Acquisition and Operational Data Center Requirements, as of August 2026 33
Table 11: Extent to Which Department of Housing and Urban Development (HUD) Addressed the Five Office of Management and Budget Acquisition and Operational Data Center Requirements, as of August 2026 34
Table 12: Extent to Which Department of the Interior Addressed the Five Office of Management and Budget Acquisition and Operational Data Center Requirements, as of August 2026 35
Table 13: Extent to Which Department of Justice Addressed the Five Office of Management and Budget Acquisition and Operational Data Center Requirements, as of August 2026 36
Table 14: Extent to Which Department of Labor Addressed the Five Office of Management and Budget Acquisition and Operational Data Center Requirements, as of August 2026 37
Table 15: Extent to Which Department of State Addressed the Five Office of Management and Budget Acquisition and Operational Data Center Requirements, as of August 2026 38

Table 16: Extent to Which Department of Transportation Addressed the Five Office of Management and Budget Acquisition and Operational Data Center Requirements, as of August 2026 39
Table 17: Extent to Which Department of the Treasury Addressed the Five Office of Management and Budget Acquisition and Operational Data Center Requirements, as of August 2026 40
Table 18: Extent to Which Department of Veterans Affairs (VA) Addressed the Five Office of Management and Budget Acquisition and Operational Data Center Requirements, as of August 2026 41
Table 19: Extent to Which Environmental Protection Agency (EPA) Addressed the Five Office of Management and Budget Acquisition and Operational Data Center Requirements, as of August 2026 42
Table 20: Extent to Which National Aeronautics and Space Administration (NASA) Addressed the Five Office of Management and Budget Acquisition and Operational Data Center Requirements, as of August 2026 43
Table 21: Extent to Which National Science Foundation (NSF) Addressed the Five Office of Management and Budget Acquisition and Operational Data Center Requirements, as of August 2026 45
Table 22: Extent to Which Nuclear Regulatory Commission (NRC) Addressed the Five Office of Management and Budget Acquisition and Operational Data Center Requirements, as of August 2026 46
Table 23: Extent to Which Office of Personnel Management (OPM) Addressed the Five Office of Management and Budget Acquisition and Operational Data Center Requirements, as of August 2026 47
Table 24: Extent to Which Small Business Administration (SBA) Addressed the Five Office of Management and Budget Acquisition and Operational Data Center Requirements, as of August 2026 48
Table 25: Extent to Which Social Security Administration (SSA) Addressed the Five Office of Management and Budget Acquisition and Operational Data Center Requirements, as of August 2026 49

Abbreviations

CFO Act	Chief Financial Officers Act of 1990
CIO	Chief Information Officer
DCIM	Data Center Infrastructure Management
DCOI	Data Center Optimization Initiative
DHS	Department of Homeland Security
DOD	Department of Defense
EPA	Environmental Protection Agency
FAA	Federal Aviation Administration
FDCCI	Federal Data Center Consolidation Initiative
FDCEA	Federal Data Center Enhancement Act
FISMA	Federal Information Security Modernization Act
FITARA	Federal Information Technology Acquisition Reform Act
GSA	General Services Administration
HHS	Department of Health and Human Services
HUD	Department of Housing and Urban Development
IT	information technology
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
SSA	Social Security Administration
TCSC	Treasury Common Services Center
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.

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

November 18, 2026

The Honorable Rand Paul, M.D.
Chairman
The Honorable Gary C. Peters
Ranking Member
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable James Comer
Chairman
The Honorable Robert Garcia
Ranking Member
Committee on Oversight and Government Reform
House of Representatives

Federal agencies use data centers and cloud applications for their mission-critical data and operations. Data centers house computer servers, data storage systems, and network equipment that provide digital applications and services—such as artificial intelligence and cloud computing.[1] Agencies are increasingly using digital services to make key processes more efficient, accessible, and scalable. The growing use of artificial intelligence among agencies will further increase demand for high-performance computing provided by data centers.

In December 2023, Congress, recognizing the growing need to ensure that data centers and cloud applications meet high standards for cybersecurity, resiliency, and availability, passed the Federal Data Center Enhancement Act (FDCEA), as part of the National Defense Authorization Act for Fiscal Year 2024.[2] The FDCEA required, among other things, the Office of Management and Budget (OMB) to establish minimum requirements for new data centers and issue guidance for the 24 Chief

[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 (e.g., networks, servers, storage applications, and services) that can be rapidly provisioned and released.

[2]FDCEA modified the statutory authorization for the Federal Data Center Consolidation Initiative (now known as the Federal Data Center Optimization Initiative) under section 834 of the Federal Information Technology Acquisition Reform Act (FITARA), Pub. L. No. 113-291, division A, title VIII, subtitle D, 128 Stat. 3292, 3444 – 3448 (Dec. 19, 2014) (44 U.S.C. § 3601 note). FDCEA extended the sunset date to October 1, 2026. Pub. L. No. 118-31, division E, title LIII, 137 Stat. 136, 940 (Dec. 22, 2023) (44 U.S.C. § 3601 note).

Financial Officers Act of 1990 (CFO Act) agencies to incorporate the requirements into the operations of their existing data centers.[3]

The FDCEA also included a provision for GAO to annually review and verify the compliance of federal agencies with OMB's requirements for new and existing data centers. This third and final annual review responded to that statutory requirement.[4] Our objective was to determine the extent to which federal agencies have incorporated OMB's acquisition and operational requirements for data centers.

To address this objective, we sought information from the 24 CFO Act agencies. Three out of the 24 agencies (Department of Education, General Services Administration, and the U.S. Agency for International Development) stated that they do not have any data centers. As a result, they were not included in the analysis of compliance with OMB requirements. We analyzed OMB's implementation guidance for the FDCEA, Memorandum M-25-03, issued on January 14, 2025, to identify the five requirements for federal agencies to incorporate when acquiring and operating agency-operated and contractor-operated data centers. We requested relevant data center documentation from all 21 agencies and analyzed the documentation, including policies, procedures, and risk management and security plans, from the agencies that provided it. In some cases, the agencies did not have the requested information. In addition, we obtained and analyzed responses from each of the 21 agencies to semi-structured questions describing each agency's number of data centers and efforts to incorporate OMB's requirements into their

[3]Unless otherwise noted, these requirements applied to the 24 federal agencies covered by FDCEA § 5302 (corresponding to the same agencies covered by the Federal Data Center Consolidation Initiative (now known as the Federal Data Center Optimization Initiative) in section 834(a)(2) of the Federal Information Technology Acquisition Reform Act (FITARA). The 24 agencies are the Departments of Agriculture, Commerce, Defense (DOD), Education, Energy, Health and Human Services (HHS), Homeland Security (DHS), Housing and Urban Development (HUD), the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs (VA); and the 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 U.S. Agency for International Development. These are also the same 24 departments and major agencies covered by the Chief Financial Officers Act of 1990, 31 U.S.C. § 901(b).

[4]This is the third and final of the three reviews, because the provisions of the FDCEA expired on October 1, 2026. The first review in 2024 and second review in 2025 resulted in briefings to congressional staff members on the status of OMB's efforts to develop operational requirements and guidance for federal data centers and agencies' efforts to incorporate these requirements.

data centers. We then compared agency documentation and responses to the requirements outlined in OMB Memorandum M-25-03. Specifically, we determined whether the evidence provided by the agencies addressed the evaluation criteria for each requirement. To determine an overall rating for each of the five requirements, we summarized the results of our assessments as:

- fully addressed—the agency fully addressed all of the requirement's evaluation criteria;
- partially addressed—the agency fully or partially addressed some, but not all, of the requirement's evaluation criteria; and
- not addressed—the agency did not address any of the requirement's evaluation criteria

We supplemented our analysis with interviews and written communication with relevant agency officials to discuss the agencies' progress in addressing these requirements, as appropriate. We also provided the results of our analysis of agency documentation to officials to corroborate our findings, collect additional evidence, and identify causes for any gaps we identified in agencies' incorporation of the requirements. A more complete description of our objective, scope, and methodology is provided in appendix I.

We conducted this performance audit from February 2026 to November 2026 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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Background

Federal data centers are expected to provide secure, reliable, and highly available computing infrastructure to enable consistent access to federal information and information systems. Acquiring and operating these centers involves managing complex computing infrastructure, extensive cooling systems, and significant energy requirements.

The specific information technology (IT) infrastructure within a data center varies depending on the types of digital applications and services the data center supports. Generally, a data center contains servers, data storage drives, and networking equipment. The servers contain the hardware

responsible for large-scale computing power, and some data center facilities contain more than 5,000 servers.

The computing equipment inside a data center generates significant heat. To ensure that the equipment runs efficiently, cooling systems work to keep temperatures and humidity within proper ranges. These cooling systems use energy to pump water, cool the air, and remove heat from the IT equipment. As a result of their computing and cooling needs, data centers require substantial amounts of energy to operate. According to one energy research organization, it is not unusual to see new data centers being built with energy needs of 100 to 1000 megawatts, roughly equivalent to powering 80,000 to 800,000 households.[5] On average, 40 to 50 percent of the energy used by a data center is for powering the IT infrastructure, and up to 40 percent is for cooling the equipment.[6]

IT Acquisition Reform Law Enhanced Data Center Consolidation and Optimization Efforts

Congress has emphasized the importance of reforming the government-wide management of IT, and in December 2014 enacted federal IT reform provisions. These provisions are commonly referred to as the Federal Information Technology Acquisition Reform Act (FITARA) and were part of the Carl Levin and Howard P. 'Buck' McKeon National Defense Authorization Act for Fiscal Year 2015.[7] Among other things, FITARA required federal agencies to:[8]

- submit to OMB a comprehensive inventory of the data centers owned, operated, or maintained by or on behalf of the agency;

[5]EPRI, *Powering Intelligence: Analyzing Artificial Intelligence and Data Center Energy Consumption* (May 28, 2024), https://www.epri.com/research/products/000000003002028905.

[6]Department of Energy, *DOE Announces $40 Million for More Efficient Cooling for Data Centers* (May 9, 2023), https://www.energy.gov/articles/doe-announces-40-million-more-efficient-cooling-data-centers.

[7]Pub. L. No. 113-291, division A, title VIII, subtitle D, 128 Stat. 3292, 3438 (Dec. 19, 2014).

[8]Pub. L. No. 113-291 § 834, 128 Stat. 3444–48 (44 U.S.C. 3601 note). Unless otherwise noted, these requirements apply to the 24 agencies specified in section 834 (corresponding to those agencies covered by the Chief Financial Officers Act of 1990. 31 U.S.C. § 901(b)).

- submit a multi-year strategy to achieve the consolidation and optimization of the agency's data centers,[9] to include performance metrics consistent with government-wide data center consolidation and optimization metrics; and
- report to OMB, on a quarterly basis, progress toward meeting government-wide data center consolidation and optimization metrics.

Additionally, the Federal Chief Information Officer (CIO) within OMB was tasked with establishing metrics for data center consolidation and optimization, ensuring public access to agencies' progress, and developing annual goals for cost savings and optimization improvements through OMB's Federal Data Center Consolidation Initiative (FDCCI).[10]

In August 2016, OMB issued Memorandum M-16-19, which established the Data Center Optimization Initiative (DCOI) and included guidance on how to implement the data center consolidation and optimization provisions of FITARA.[11] In June 2019, OMB issued Memorandum M-19-19, which updated the DCOI and redefined a data center as a purpose-built, physically separate, dedicated space that meets certain criteria.[12] The memorandum also directed agencies to focus their efforts on their tiered data centers and to stop reporting on spaces not designed to be data centers (i.e., non-tiered data centers) as part of their inventory.[13] The

[9]In lieu of submitting a data center inventory and strategy, the Department of Defense could submit this information as part of a defense-wide plan and report on cost savings, as required under §§ 2867(b)(2) and 2867(d) of the *National Defense Authorization Act for Fiscal Year 2012*.

[10]The sunset date for the data center provisions of FITARA was extended to October 1, 2022, and the statutory authorization for the provision has now lapsed. 44 U.S.C. 3601 note. The Federal Data Center Enhancement Act extended the sunset date to October 1, 2026.

[11]Office of Management and Budget, *Data Center Optimization Initiative (DCOI)*, Memorandum M-16-19 (Washington, D.C.: Aug. 1, 2016).

[12]Office of Management and Budget, *Update to Data Center Optimization Initiative (DCOI)*, Memorandum M-19-19 (Washinton, D.C.: June 25, 2019). According to OMB Memorandum M-19-19 and related reporting instructions, a data center generally is a purpose-built, physically separate, and dedicated space that contains one or more racks of servers, mainframes, and/or high-performance computers; has a dedicated uninterruptable power supply and/or backup generator for prolonged power outages; and/or has a dedicated cooling system or zone. Agencies are to report facilities matching these criteria as tiered data centers.

[13]OMB derived the term "tiered" and its definition from the Uptime Institute's Tier Classification System. However, OMB notes that no specific certification is required in order for a data center to be considered tiered by OMB. According to OMB M-16-19, all data centers not marked as tiered should be considered non-tiered.

guidance outlined a process by which agencies could request, and OMB would approve, that these facilities no longer be reported.

Prior GAO Reporting on Data Center Consolidation and Optimization Resulted in Billions in Savings

Since 2016, we have reported on OMB's DCOI requirements for agencies and made recommendations to improve OMB's oversight of DCOI.[14] In addition, since the enactment of FITARA, we have annually reviewed agencies' efforts to implement the data center provisions of FITARA and have published reports documenting the findings from each of these reviews.[15] We noted that, while agencies were reporting progress toward DCOI data center closure, cost savings, and optimization goals, many agencies had incomplete optimization plans and were not meeting those goals. We made 126 recommendations from 2016 to 2021. Of the 126 recommendations, 101 have been implemented; 19 have been closed as not implemented; five were no longer valid; and one remains open. Specifically, as of July 2026, one recommendation to OMB related to revising its prior guidance to show agencies how to measure server utilization remains open.[16] In February 2023, we reported that agencies had realized a cumulative total of $6.6 billion in cost savings and avoidances from fiscal years 2012 through 2021 related to data center consolidation and optimization.[17]

[14]GAO, *Data Center Consolidation: Agencies Making Progress, but Planned Savings Goals Need to Be Established [Reissued on March 4, 2016]*, GAO-16-323 (Washington D.C.: Mar. 3, 2016); *Data Center Consolidation: Reporting Can Be Improved to Reflect Substantial Planned Savings*, GAO-14-713 (Washington, D.C.: Sept. 25, 2014); *Data Center Consolidation: Strengthened Oversight Needed to Achieve Cost Savings Goal*, GAO-13-378 (Washington, D.C.: Apr. 23, 2013); *Data Center Consolidation: Agencies Making Progress on Efforts, but Inventories and Plans Need to Be Completed*, GAO-12-742 (Washington, D.C.: July 19, 2012); and GAO-11-565.

[15]GAO, *Data Center Optimization: Agencies Continue to Report Mixed Progress Against OMB's Targets*, GAO-22-105118 (Washington, D.C.: Mar. 8, 2022); *Data Center Optimization: Agencies Report Progress, but Oversight and Cybersecurity Risks Need to Be Addressed,* GAO-20-279 (Washington, D.C.: Mar. 5, 2020); *Data Center Optimization: Additional Agency Actions Needed to Meet OMB Goals*, GAO-19-241 (Washington, D.C.: Apr. 11, 2019); *Data Center Optimization: Continued Agency Actions Needed to Meet Goals and Address Prior Recommendations*, GAO-18-264 (Washington, D.C.: May 23, 2018); *Data Center Optimization: Agencies Need to Address Challenges and Improve Progress to Achieve Cost Savings Goal*, GAO-17-448 (Washington, D.C.: Aug. 15, 2017); *Data Center Optimization: Agencies Need to Complete Plans to Address Inconsistencies in Reported Savings*, GAO-17-388 (Washington, D.C.: May 18, 2017); and GAO-16-323.

[16]GAO, *Data Center Optimization: Agencies Report Progress and Billions Saved, but OMB Needs to Improve Its Utilization Guidance*, GAO-21-212 (Washington, D.C.: Mar. 4, 2021).

[17]GAO, *Data Center Optimization: Agencies Continue to Report Progress*, GAO-23-105946 (Washington, D.C.: Feb. 27, 2023).

Federal Data Center Enhancement Act of 2023 Called for OMB to Establish Minimum Requirements and Issue Implementation Guidance

While the FITARA requirements led to the consolidation and optimization of federal data centers, the FDCEA of 2023 shifted the focus to ensuring high standards of cybersecurity, resiliency, and availability for the centers that remain.

Congress acknowledged, in enacting the FDCEA, that the needs of the federal government with respect to data access and data processing systems have evolved since 2014. Given the significant efficiencies already achieved under FDCCI, Congress did not renew the expired provisions. Instead, it enacted the FDCEA, which struck the FDCCI provisions, and, among other things, directed OMB to set requirements for federal data centers to meet appropriate standards for cybersecurity, resiliency, and availability.

Specifically, the FDCEA required the following, among other things:

- The Administrator of the Office of Electronic Government within OMB (the Federal CIO) was to establish minimum requirements for new data centers, in consultation with the Administrator of General Services (i.e., head of the General Services Administration (GSA)), Director of the Cybersecurity and Infrastructure Security Agency within the Department of Homeland Security, National Cyber Director, and Federal CIO Council, by June 19, 2024.[18] These minimum requirements were to include the following areas:
  - ensuring the availability of new data centers
  - evaluating the use of new data centers, focusing on facility costs, energy consumption, and related infrastructure
  - establishing required uptime percentages[19]
  - implementing protections against power failures, including on-site energy generation and access to multiple transmission paths
  - ensuring protections against physical intrusions and natural disasters

[18]In our 2024 briefing to congressional staff members, we reported that OMB officials stated that they met with the General Services Administration Office of Government-wide Policy, Cybersecurity and Infrastructure Security Agency Interagency Security Committee, Federal Chief Information Officer Council, and Office of the National Cyber Director to discuss the development of data center requirements, as required by the Federal Data Center Enhancement Act.

[19]Uptime percentage is calculated as the number of available hours minus unplanned downtime.

- complying with information security protections as mandated by applicable laws and policy[20]
- incorporating any other requirements deemed appropriate by OMB

- OMB was to issue guidance, as appropriate, for the 24 CFO Act agencies to incorporate the requirements into the operations of any data centers by September 17, 2024.
- The 24 CFO Act agencies were to notify OMB and Congress during the development and planning lifecycle of new data centers and use technology in determining whether to establish new data centers or continue to operate an existing data center.
- OMB was to maintain a public-facing website that included information, data, and explanatory statements relating to the compliance of the 24 CFO Act agencies with these requirements. In maintaining the website, OMB was required to ensure that these agencies regularly, and not less frequently than biannually, updated the information related to their data centers.[21]

The provisions of the FDCEA sunset on October 1, 2026.

OMB's Memorandum Established Requirements and Guidance for Acquiring and Operating Federal Data Centers

In January 2025, OMB issued Memorandum M-25-03, establishing both the minimum requirements and the implementation guidance to federal agencies related to the FDCEA.[22] The memorandum was issued approximately seven months after the June 19, 2024, statutory deadline to establish requirements, and approximately four months after the September 17, 2024, deadline to issue implementation guidance. The memorandum established updated standards for the acquisition, design, and management of federal data centers and centralized agency data center investment decisions.

In this memorandum, OMB defined that a data center was (1) composed of one or more permanent or semi-permanent structures, or a dedicated space within such a structure, that operates persistently in a fixed

[20]Subchapter II of chapter 35 of title 44, United States Code, establishes federal information security requirements, as enacted by the Federal Information Security Modernization Act of 2014.

[21]The last update on OMB's public-facing website was July 2025. As of August 2026, there is no public-facing website with updates.

[22]Memorandum M-25-03 superseded prior data center policies, including the now-expired Data Center Optimization Initiative (DCOI).

location; (2) used for the housing of IT equipment, including servers, mainframe computers, high-performance computing devices, or data storage devices; and (3) actively used for the hosting of information and information systems that are accessed by other systems or by users on other devices.

The guidance further stated that it applied to agency-operated and contractor-operated data centers. Specifically, a data center was considered agency-operated if it was owned, operated, or maintained directly by a covered agency. This included facilities leased directly by an agency or those occupied under a General Services Administration occupancy agreement. A data center was considered contractor-operated if it was owned, operated, or maintained by a contractor on behalf of a covered agency. Contractor-operated data centers could include commercial co-location, in which an agency is one among many tenants.

Furthermore, the guidance also specified that some provisions of the memorandum applied differently depending on whether a given data center was new or existing.[23] A data center was considered new if it was established or substantially upgraded or expanded after the date of the memorandum, January 14, 2025. Substantial upgrades or expansions were considered those involving the data center's power supply or distribution, cooling, physical security, networking, IT equipment, or size of space hosting IT equipment. If a data center did not qualify as new, then it was considered an existing data center.

The memorandum also required agencies to assess gaps in their current data center capabilities and factor those into acquisition planning. According to OMB's implementation guidance, agencies were to implement the acquisition and operational requirements into the management and planning of their data centers to ensure that federal data centers are secure, resilient, efficient, and mission ready. Table 1 describes the five OMB requirements for acquiring and operating federal data centers.

[23]OMB's memorandum applied to both new and existing data centers for four of the five requirements. For the incorporating energy and water usage into decision-making requirement, OMB did not specifically require agencies to apply the provisions to existing data centers.

Table 1: Office of Management and Budget's (OMB) Five Requirements for Acquiring and Operating Federal Data Centers

Requirement	Description
Make key data center decisions at the agency level	Given the criticality of data centers and the significant capital and ongoing investments required to acquire and manage them, agencies must centralize data center acquisition decision-making and operational management with the agency's Chief Information Officer (CIO). Centralized oversight of the agency data center footprint will ensure the agency CIO can move toward the most efficient, reliable, and secure outcomes for the agency, while integrating data center and related information technology (IT) portfolio decision-making and planning into the requisite acquisition, budget, and programmatic processes. The requiring office and the relevant procurement official should consult with the agency's CIO throughout the process of procuring a new data center or making substantial changes to an existing one. Agencies should use commercial co-location services rather than building new data centers to the extent that it is cost-effective and meets agency mission needs.
Monitor data center operations	The timely and effective operation of data centers requires regular monitoring, management, and optimization of resources by data center operators through the collection and presentation of metrics. Automated tools, such as Data Center Infrastructure Management systems, can significantly improve the efficiency of a wide range of tasks: managing physical and virtual assets, monitoring equipment and power usage, metering energy consumption, and performing other core operational and planning functions. Use of automated tools and the data that they provide can reduce the costs associated with data centers. Agencies must incorporate automated tools, such as Data Center Infrastructure Management systems, into the management of all new data centers, including tools that monitor facilities-related data such as electrical consumption. For existing data centers, agencies should adopt the use of such tools to the extent that it is cost-effective.
Incorporate energy and water usage into decision-making	Data centers consume significant amounts of energy and water to power and cool IT equipment. As such, the cost, scarcity, and environmental impact of energy and water consumption necessitates that agencies evaluate data centers against resource consumption metrics and best practices when making their decisions. Improved efficiency can reduce overall costs and increase reliability of data centers. While designing or planning a new data center, including any substantial upgrades to an existing data center, agencies are required to arrange for an assessment by specialists certified in data center energy efficiency to better understand the existing data center's resource usage and recommend design considerations to achieve improved efficiencies. Agencies are required to review and consider the recommendations resulting from the assessment when making data center design or selection decisions, in coordination with the agency's Chief Sustainability Officer and the agency's facilities management representatives.
Meet mission availability requirements	To effectively enable agency missions, a data center must be able to meet the availability and uptime needs of its hosted information systems despite a variety of planned and unplanned downtime situations, such as natural disasters and equipment failure. Agencies shall adopt a risk management-based approach to identify, reduce the likelihood of, and mitigate risks to the availability of data centers using frameworks such as National Institute of Standards and Technology[a] Special Publications. This approach includes implementing an internal control policy to determine and meet data center availability (uptime) requirements using the results of a business impact analysis.[b]

Requirement	Description
Meet information and physical security requirements	Data centers must be able to meet the reliability and resiliency needs of their hosted information and information systems through implementation of appropriate information security and physical security protections. Effective implementation of the Federal Information Security Modernization Act[c] (FISMA), including the appropriate use of National Institute of Standards and Technology frameworks and security controls, should guide agencies in protecting the information and information systems stored within a data center. Information systems used by a contractor to manage a data center should comply with the appropriate agency policy for managing risk in accordance with FISMA requirements. For both new and existing data centers, agencies must follow the Interagency Security Committee[d] risk management process to determine the physical security needs for each data center facility and to implement the appropriate standards for countermeasures. To complete the risk management process for physical security of the data center facility, agency CIOs must work in coordination with other senior officials for security and facilities management within their agency.

Source: GAO analysis of OMB Memorandum M-25-03. I GAO-27-108971

[a]The National Institute of Standards and Technology is the federal agency that develops information security standards and guidelines for federal information systems.

[b]According to OMB Memorandum M-25-03, a business impact analysis identifies the impacts of information system downtime on agency missions and is part of an agency's contingency planning processes, and relevant customer experience to determine the maximum tolerable duration and frequency of downtime events for each of the information sets and information systems hosted in a data center.

[c]FISMA is a federal statute that establishes the framework for protecting federal information systems and requires agencies to develop, document, and implement agencywide information security programs. It also assigns agency heads the ultimate authority and responsibility to develop and implement agencywide information security programs.

[d]The Interagency Security Committee is an interagency body that develops policies and standards for the security of nonmilitary federal facilities, while the Department of Defense has incorporated applicable standards into its facility-security policies and Unified Facilities Criteria.

OMB required agencies to have satisfied the five requirements for new and existing agency-operated data centers by January 14, 2026. For contractor-operated centers, compliance was expected by the later of the following two dates, (1) January 14, 2026, or (2) the date after January 14, 2025, that the contract was first renewed, extended, or replaced.[24] The provisions in the OMB memorandum expired on September 30, 2026.

Agencies Reported the Number of New and Existing Data Centers

The 24 CFO Act agencies reported the number of federal data centers they had as of March 2026. Three agencies (Education, GSA, and the U.S. Agency for International Development) reported that they had no new or existing data centers. The 21 remaining agencies collectively reported 1,392 data centers, of which 1,217 were agency-operated, 168 were contractor-operated, and seven were new.

[24]For contractor-operated data centers, the majority of agencies reported that compliance was expected by January 14, 2026.

Of the 21 agencies with data centers,

- Ten agencies (Department of Agriculture, Department of Defense (DOD), Department of Energy, Department of Health and Human Services (HHS), Department of Homeland Security (DHS), Department of the Interior, Department of Justice, Department of the Treasury, Department of Veterans Affairs (VA), and Office of Personnel Management (OPM)) reported having both agency and contractor-operated data centers;
- Three agencies (Department of Housing and Urban Development (HUD), National Science Foundation (NSF), and Small Business Administration (SBA)[25]) reported having no agency-operated data centers;
- Eight agencies (Department of Commerce, Department of Labor, Department of State, Department of Transportation, Environmental Protection Agency (EPA), National Aeronautics and Space Administration (NASA),[26] Nuclear Regulatory Commission (NRC), and Social Security Administration (SSA)) reported having no existing contractor-operated data centers.

In addition, five agencies (Agriculture, Commerce, Energy, HHS, and NRC) reported having new data centers. For example, Commerce officials noted that it had a new contractor-operated data center. DOD reported that it was still determining whether it would have new data centers.[27]

Table 2 shows the agency-reported information on the number of existing agency-operated and contractor-operated data centers, and new data centers.

[25]In July 2026, SBA officials reported that all data centers are expected to close by the end of October 2026.

[26]According to NASA officials, it counted only agency-operated real property facilities with data hall rooms. During fiscal year 2026, the agency stated it plans to conduct a survey to identify any additional facilities that meet the OMB definition based on OMB M-25-03 and update its inventory accordingly.

[27]As of August 2026, DOD officials did not provide an update on the status of the number of new data centers.

Table 2: Agency-Reported Number of Existing and New Data Centers, as of March 2026

	Number of existing data centers		Number of new data centers[a]
Agency	**Agency-operated**	**Contractor-operated**	
Department of Agriculture[b]	1	1	1
Department of Commerce	46	0	1
Department of Defense	477	11	To be determined
Department of Education	0	0	0
Department of Energy	28	79	1
Department of Health and Human Services	149	12	2
Department of Homeland Security	3	11	0
Department of Housing and Urban Development	0	2	0
Department of the Interior	43	16	0
Department of Justice	9	4	0
Department of Labor	6	0	0
Department of State	140	0	0
Department of Transportation	16	0	0
Department of the Treasury	21	24	0
Department of Veterans Affairs[c]	250	2	0
Environmental Protection Agency	2	0	0
General Services Administration	0	0	0
National Aeronautics and Space Administration	17	0	0
National Science Foundation	0	1	0
Nuclear Regulatory Commission	4	0	2
Office of Personnel Management	1	1	0
Small Business Administration[d]	0	4	0
Social Security Administration	4	0	0
U.S. Agency for International Development	0	0	0
Total	**1217**	**168**	**7**

Source: GAO analysis of agency-provided data. I GAO-27-108971

[a]Agencies reported that the new data centers included either agency-operated or contractor-operated data centers.

[b]Department of Agriculture officials stated that the agency will no longer have a federally owned data center after calendar year 2027.

[c]Department of Veterans Affairs officials reported that the agency plans to close one of its existing contractor-operated data centers by November 30, 2026.

[d]Small Business Administration officials stated that the agency plans to close all data centers by the end of October 2026.

Federal Agencies Varied in Incorporating OMB's Acquisition and Operational Requirements for Their Data Centers

OMB's memorandum issued in January 2025 established minimum requirements for acquiring and operating federal data centers as well as guidance for implementing the requirements. The five requirements for agencies to address were to (1) make key data center decisions at the agency level, (2) monitor data center operations, (3) incorporate energy and water usage into decision-making, (4) meet mission availability requirements, and (5) meet information security and physical security requirements. As noted above, OMB required agencies to satisfy these requirements by January 14, 2026, with potentially later dates for contractor-operated data centers. The requirements in the memorandum expired on September 30, 2026.

Agencies varied in incorporating OMB's five acquisition and operational requirements into the management and planning of their data centers.[28] Specifically, as of August 2026, while none of the 21 agencies with reported data centers fully addressed all five requirements, nine agencies fully addressed half or more of the applicable requirements and 19 partially or fully addressed all of the applicable requirements.

Table 3 reflects the extent to which the 21 agencies with data centers incorporated the five acquisition and operational requirements into their data centers as of August 2026. In addition, appendix II provides more details on the assessment of each of the 21 agencies.

Table 3: Extent to Which Federal Agencies Incorporated the Office of Management and Budget's Five Acquisition and Operational Requirements for their Data Centers, as of August 2026

Agency	Make key data center decisions at the agency level	Monitor data center operations	Incorporate energy and water usage into decision-making	Meet mission availability requirements	Meet information and physical security requirements
Department of Agriculture	◐	◐	◐	◐	◐
Department of Commerce	◐	◐	◐	◐	◐
Department of Defense	●	●	—	◐	◐
Department of Energy	◐	◐	◐	◐	◐

[28]Twenty-one agencies reported data centers and three agencies reported that they did not have data centers. The five OMB requirements were not applicable to those three agencies: Education, GSA, and the U.S. Agency for International Development.

Agency	Make key data center decisions at the agency level	Monitor data center operations	Incorporate energy and water usage into decision-making	Meet mission availability requirements	Meet information and physical security requirements
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	◐	●	—	◐	◐
National Aeronautics and Space Administration	◐	◐	—	◐	◐
National Science Foundation	◐	◐	—	◐	◐
Nuclear Regulatory Commission	●	●	◐	◐	●
Office of Personnel Management	◐	◐	—	◐	◐
Small Business Administration	◐	○	—	◐	◐
Social Security Administration	●	●	—	●	◐

● = Fully addressed—the agency fully addressed all of the requirement's evaluation criteria.

◑ = Partially addressed—the agency fully or partially addressed some, but not all, of the requirement's evaluation criteria.

○ = Not addressed—the agency did not address any of the requirement's evaluation criteria.

— = The requirement did not apply to the agency as it reported it had no new data centers and because the Office of Management and Budget did not specifically require agencies to apply the requirement to existing data centers.

Source: GAO analysis of agency documentation. | GAO-27-108971

Note: The Office of Management and Budget required existing data centers to comply with some of the requirements only as practical or not at all. The Federal Data Center Enhancement Act directed that OMB "shall issue guidance to ensure, as appropriate, that covered agencies incorporate the minimum requirements established [for new data centers] into the operations of any data center for a covered agency existing as of the day of enactment [of the Act]."

Make key data center decisions at the agency level. Ten agencies fully addressed the requirement and 11 partially addressed the requirement. The 10 agencies that fully addressed the requirement were DOD, DHS, Interior, Justice, Labor, State, Transportation, Treasury, NRC, and SSA. For example, according to Interior's *Departmental Manual Part 112 Chapter 24* and *Hosting Services Policy* documents, data center acquisition decision-making and operational management are centralized with the Chief Information Officer (CIO), and the requiring office and procurement official coordinate with the CIO throughout the budget and acquisition process.

The 11 agencies that partially addressed the requirement were Agriculture, Commerce, Energy, HHS, HUD, VA, EPA, NASA, NSF, OPM, and SBA. For example:

- According to Energy officials, the agency has established an enterprise governance framework through which the CIO is actively engaged in the planning, budgeting, and execution of all IT acquisitions. However, these officials reported that 29 percent of Energy's data centers had no CIO involvement. Energy officials said that these data centers operate under a decentralized governance structure in which program offices, rather than the centralized CIO organization, oversee IT management. Therefore, the agency has not sufficiently demonstrated that the requiring office and the relevant procurement official consult with the agency's CIO throughout the process of procuring a new data center or making substantial changes to an existing one.
- HUD officials stated that the agency has centralized data center acquisition decision-making and operational management under its CIO. However, the documentation HUD provided did not demonstrate that the CIO is making key data center decisions at the agency level.

Monitor data center operations. Ten agencies fully addressed the requirement, nine partially addressed the requirement, and two did not address it.[29] The agencies that fully addressed this requirement were

[29]DOD reported that the number of new data centers was to be determined. Therefore, we did not assess whether the agency incorporated automated tools into the management of all new data centers.

DOD, DHS, HUD, Labor, Justice, State, Transportation, EPA, NRC, and SSA. For example, for its existing data centers, according to the DOD Data Center Optimization Initiative memorandum, the Data Center Infrastructure Management (DCIM) system is the agency's authoritative database for data center inventory reporting. It captures the current disposition of data center assets to include the type, location, size, and total physical and virtual server counts.

Nine agencies (Agriculture, Commerce, Energy, HHS, Interior, VA, NASA, NSF, and OPM) partially addressed this requirement. For example:

- While Commerce has draft memorandums that describe three of its components' approaches to implementing monitoring capabilities for new and existing data centers, agency officials stated that the agency is issuing a Data Center Policy Memorandum. The memorandum will mandate the adoption of automated monitoring tools—including the DCIM systems—and set agencywide minimum monitoring standards for both new and existing data centers.[30]
- HHS provided examples of how its components incorporate automated tools, such as the DCIM systems, into the management of its data centers, including tools that monitor facilities-related data such as electrical consumption. However, the one component, Centers for Medicare & Medicaid Services, that reported new data centers did not provide any supporting documentation to demonstrate how the agency incorporated these tools into the management of the new data centers. Additionally, for its existing data centers, HHS did not provide supporting documentation demonstrating its use of such tools to the extent that it was cost-effective.
- For its existing data centers, NASA stated that it uses the DCIM system and other tools to monitor data centers. Also, the NASA CIO has funded implementation of a standard enterprise DCIM solution with centralized monitoring capabilities but has not yet implemented the enterprise solution. The agency expects to implement this solution in calendar year 2026, and a detailed project plan is currently being developed. According to NASA officials, DCIM is only required for new or substantially upgraded centers. However, the OMB requirement stated that for existing data centers, agencies should adopt the use of

[30]On October 16, 2026, while the report was at the agency for comment, the department finalized its data center policy to address compliance gaps and optimization, and strengthen alignment with OMB's requirements, among other things. According to the policy, operating units and offices are required to implement the five OMB requirements, including the adoption of automated monitoring tools, within 90 business days.

such tools to the extent that it is cost-effective. NASA reported that it had no new data centers. Therefore, we did not assess whether the agency incorporated automated tools into the management of all new data centers. NASA officials did state that the agency plans to incorporate automated tools into the management of any new data centers approved in the future.

The remaining two agencies (Treasury and SBA) did not address this requirement. According to Treasury officials, operational monitoring is conducted through enterprise services and the bureau level management of data center environments, but the agency did not state whether it adopted the use of automated tools to do so. Additionally, SBA officials stated that it did not address this requirement because OMB's memorandum was only related to new data centers. As previously mentioned, OMB's guidance stated that for existing data centers, agencies should adopt the use of such tools to the extent that it is cost-effective.

Incorporate energy and water usage into decision-making. Five agencies (Agriculture, Commerce, Energy, HHS, and NRC) reported having new data centers, and all five partially addressed this requirement. For example:

- Agriculture relies on the *System and Organization Controls for Service Organizations* report for its contractor-operated data center. This report provides independent assurance over controls governing the contractor's use of the DCIM system to facilitate the exchange and analysis of data from energy; lightning; fire safety; and heating, ventilation, and air conditioning systems. Agriculture officials also stated that the agency utilizes DCIM tools for monitoring energy usage in agency-operated data centers and incorporates data into decision-making. However, the department did not provide documentation to demonstrate that while designing its new data center, the agency arranged for an assessment by specialists certified in data center energy efficiency.
- NRC provided documentation identifying a certified Data Center Energy Practitioner currently employed by NRC. This individual serves as the Administrative Contracting Officer's Representative for the Equinix co-location contracts and as the Office of the Chief Information Officer's technical advisor for all data center-related projects. Additionally, NRC described how it considered an existing data center's resource usage when making its design and selection decisions. However, the agency did not demonstrate how it

coordinates with the agency's Chief Sustainability Officer and the agency's facilities management representatives when reviewing and considering the assessment recommendations.

Sixteen agencies (DOD, DHS, HUD, Interior, Justice, Labor, State, Transportation, Treasury, VA, EPA, NASA, NSF, OPM, SBA, and SSA) reported that they did not have any new data centers for this reporting period, and thus, we did not assess their compliance for this requirement. Nonetheless, 13 agencies reported incorporating energy and water usage into decision-making for their existing data centers, even though OMB did not specifically require agencies to do so.

Meet mission availability requirements. Two agencies fully addressed the requirement, and the remaining 19 partially addressed the requirement. The agencies that fully addressed the requirement were Justice and SSA. For example, Justice's *Cybersecurity Program* order and *Information System Contingency Plan* require components to define system availability requirements, implement contingency planning, and manage risks to ensure the availability and continuity of mission-critical information systems, which include data centers. Additionally, according to Justice's *Data Center Actions Information Technology Action* memorandum, component CIOs operating data centers must establish a target availability of 99.8 percent for their data centers and report actual availability for the data centers on a semi-annual basis through a data call. The memorandum notes that risks affecting each data center's availability must be identified and mitigated in accordance with Justice's *Information Systems Contingency Planning Guide*.

Nineteen agencies (Agriculture, Commerce, DOD, Energy, HHS, DHS, HUD, Interior, Labor, State, Treasury, Transportation, VA, EPA, NASA, NSF, NRC, OPM, and SBA) partially addressed this requirement. For example:

- VA officials stated that the agency manages risk through a continuous authorization monitoring process that allows for the processing of risk management framework items such as authorities to operate and plans of action and milestones. While VA established a policy

directive[31] and guidance[32] that govern its foundational cybersecurity requirements, these documents did not describe how the agency is using the results of a business impact analysis to set minimum availability requirements for each data center that will meet the availability needs of its hosted information and information systems.

- State officials stated that its data centers meet availability requirements, and that the agency follows standards to minimize planned downtime to meet mission availability requirements and has adopted modern software development practices, such as cloud services. According to State officials, business impact analyses are conducted as part of the authorization to operate process. State also described how it conducts these business impact analyses. However, it did not sufficiently demonstrate that the agency has an internal control process for managing risks to data center availability, including using the results of a business impact analysis to set minimum availability requirements for all its data centers that will meet the availability needs of its hosted information and information systems.
- According to EPA officials, data center customers maintain signed business impact assessment statements and contingency plans that are updated annually. The agency also uses system security plans to identify and mitigate controls. However, the agency did not demonstrate that it is using the results of a business impact analysis to set minimum availability requirements for each data center that will meet the availability needs of its hosted information and information systems.

Meet information and physical security requirements. Four agencies fully addressed the requirement, and the remaining 17 partially addressed it. The agencies that fully addressed the requirement were DHS, State, Treasury, and NRC. For example, DHS's *Instruction Manual 121-01-010-01 Physical Security* describes how the agency meets physical security requirements, including how it uses an Interagency Security Committee risk management process and communicates with others, such as the Chief Security Officer, Facility Security Committee, and physical security officials, to complete the process for physical security of data center facilities. Additionally, its security and privacy plan describes controls on securing information and physical facilities of data centers. These include

[31]Department of Veterans Affairs, *VA Cybersecurity Program*, VA Directive 6500 (Washington, D.C.: Feb. 24, 2021).

[32]Department of Veterans Affairs, *Risk Management Framework for VA Information Systems VA Information Security Program,* VA Handbook 6500 (Washington, D.C.: Feb. 24, 2021).

its CIO working in coordination with other senior officials for security and facilities management within the agency to complete the Interagency Security Committee risk management process.

Seventeen agencies (Agriculture, Commerce, DOD, Energy, HHS, HUD, Interior, Justice, Labor, Transportation, VA, EPA, NASA, NSF, OPM, SBA, and SSA) partially addressed this requirement. These agencies reported that information systems used by a contractor to manage a data center comply with the appropriate agency policy for managing risks in accordance with FISMA requirements. These agencies also reported that they follow the Interagency Security Committee risk management process to determine the physical security needs for each data center facility and to implement the appropriate standards for countermeasures. However, these agencies either did not provide documentation or it was not sufficient to demonstrate that the CIO works in coordination with other senior officials for security and facilities management within their agency to complete the Interagency Security Committee risk management process for both new and existing data centers.

While most of the 21 agencies in our review stated that they believed they had addressed all five of OMB's acquisition and operational requirements for their data centers, they did not provide evidence of full compliance. GAO is not making recommendations to the agencies because the OMB requirements expired on September 30, 2026, and the underlying FDCEA provisions sunset on October 1, 2026. Congress has introduced a variety of legislative proposals for data centers nationwide that are intended to, among other things, address data center energy use reporting and environmental requirements; electric grid, environmental, and public-health impacts of data centers; disclosure requirements for artificial intelligence data center development and site selection; and energy and water use reporting for large data centers. Although these legislative proposals apply more broadly to data centers nationwide, they may also impact federal data centers going forward. Moreover, since 2023 when the FDCEA was enacted, the demand for data storage and processing capacity, especially for artificial intelligence development and deployment, has increased. If Congress puts forth legislation to reauthorize or replace the FDCEA, it will have the opportunity to direct OMB to update the minimum acquisition and operational requirements for agencies to encourage continued focus on enhancing the cybersecurity, resiliency, and availability of new and existing federal data centers.

Conclusions

Congress has introduced various legislative proposals to make a variety of changes that would affect data centers nationwide. Such changes are

complex, and the effects will vary based on the specific proposals. These legislative proposals may also have impacts on federal data centers. Moreover, since FDCEA was enacted in 2023, the current IT landscape has changed. The Act's provisions sunset on October 1, 2026. Advances in artificial intelligence capabilities and its growing use among agencies have further increased demand for high-performance computing provided by data centers. Congress may prefer to reauthorize or replace FDCEA with new priority areas focused on broader modernization or cloud service requirements. In doing so, it would be important to review and update the minimum OMB requirements as appropriate. This report provides key insights into current federal data center acquisition and operational practices to inform Congress if it contemplates any changes to the management of federal data centers.

Matter for Congressional Consideration

Congress should consider reauthorizing the FDCEA or replacing it with a new law reflecting updated priorities and OMB's acquisition and operational requirements for agencies' data centers. (Matter for Consideration 1)

Agency Comments

We provided a draft of this report to OMB and the 24 Chief Financial Officers Act agencies for their review and comment. We received a written letter from SSA stating that it did not have any comments—reproduced in appendix III. Six agencies—the Department of Commerce, the Department of Defense, the Department of the Treasury, National Aeronautics and Space Administration, OPM, and SSA—provided technical corrections, which we have incorporated into the report, as appropriate. Seventeen agencies (Agriculture, DHS, Education, Energy, EPA, GSA, HHS, HUD, Interior, Justice, Labor, NRC, NSF, SBA, State, Transportation, and VA) did not have any comments on our draft report. U.S. Agency for International Development did not respond because staff from the agency's Office of the Executive Secretariat reported that other agency needs had taken priority. OMB did not provide comments on our draft report.

We are sending copies of this report to the appropriate congressional committees; the Director of OMB; the Secretaries of the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Labor, State, Transportation, the Treasury, and Veterans Affairs; the U.S. Attorney General; the Administrators of the Environmental Protection Agency, General Services Administration, National Aeronautics and Space Administration, Small Business Administration, and the U.S. Agency for International Development; the Directors of the

National Science Foundation and the Office of Personnel Management; the Chairman of the Nuclear Regulatory Commission; and the Commissioner of the Social Security Administration. In addition, the report will be available at no charge on GAO's website at http://www.gao.gov.

If you or your staff have any questions about this report, please contact Carol Harris at harriscc@gao.gov. Contact points for our Offices of Congressional Relations and Media Relations may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix IV.

//SIGNED//

Carol C. Harris
Director, Information Technology and Cybersecurity

Appendix I: Objective, Scope, and Methodology

Our objective was to determine the extent to which federal agencies have incorporated the Office of Management and Budget's (OMB) acquisition and operational requirements for data centers.

The scope of our review included the 24 federal agencies covered by the Chief Financial Officers Act of 1990 that also generally corresponds to the agencies covered by the Federal Information Technology Acquisition Reform Act.[1] Three out of the 24 agencies (Department of Education, General Services Administration, and the U.S. Agency for International Development) stated that they do not have any data centers. As a result, they were not included in the analysis of compliance with OMB requirements.

To address the objective, we reviewed OMB's implementation guidance for the Federal Data Center Enhancement Act of 2023 (FDCEA), Memorandum M-25-03, to identify the five requirements for federal agencies to incorporate when acquiring and operating agency-operated and contractor-operated data centers.[2] In addition, we sought information from OMB staff in February 2026 and June 2026 on this FDCEA implementation guidance and any plans related to extending or renewing the provisions in the memorandum that expired on September 30, 2026. As of August 2026, OMB had not provided information in response to our questions.

To ensure consistent understanding and application of the requirements, we identified specific evaluation criteria in the OMB guidance that were associated with each of the five requirements. The five requirements and their associated evaluation criteria are listed in table 4.

[1]The 24 federal agencies covered by the Chief Financial Officers Act of 1990 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; 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.

[2]Office of Management and Budget, *Implementation Guidance for the Federal Data Center Enhancement Act*, M-25-03 (Washington, D.C.: Jan. 14, 2025).

Table 4: Evaluation Criteria Associated with the Office of Management and Budget's (OMB) Requirements for Acquiring and Operating Federal Data Centers

Requirement	Evaluation criteria
Make key data center decisions at the agency level	Agencies must centralize data center acquisition decision-making and operational management with the agency's Chief Information Officer (CIO). The requiring office and the relevant procurement official should consult with the agency's CIO throughout the process of procuring a new data center or making substantial changes to an existing one. Agencies should use commercial co-location services rather than building new data centers to the extent that it is cost-effective and meets agency mission needs.
Monitor data center operations	Agencies must incorporate automated tools, such as Data Center Infrastructure Management systems, into the management of all new data centers, including tools that monitor facilities-related data such as electrical consumption. For existing data centers, agencies should adopt the use of such tools to the extent that it is cost-effective.
Incorporate energy and water usage into decision-making	Agencies must evaluate data centers against resource consumption metrics and best practices when making their decisions. While designing or planning a new data center, including any substantial upgrades to an existing data center, agencies are required to arrange for an assessment by specialists certified in data center energy efficiency to better understand the existing data center's resource usage and recommend design considerations to achieve improved efficiencies. Agencies are required to review and consider the recommendations resulting from the assessment when making data center design or selection decisions, in coordination with the agency's Chief Sustainability Officer and the agency's facilities management representatives.
Meet mission availability[a]	For both new and existing data centers, agencies must have an internal control process for managing risks to data center availability that includes determining availability (uptime) requirements. Agencies must use the results of a business impact analysis, performed as part of an agency's contingency planning processes, and relevant customer experience objectives to determine the maximum tolerable duration and frequency of downtime events for each of the information sets and information systems hosted in a data center. Using the results of that analysis, agencies must then set minimum availability requirements for each data center that will meet the availability needs of its hosted information and information systems.
Meet information and physical security	Information systems used by a contractor to manage a data center should comply with the appropriate agency policy for managing risk in accordance with Federal Information Security Modernization Act requirements. For both new and existing data centers, agencies must follow the Interagency Security Committee risk management process to determine the physical security needs for each data center facility and to implement the appropriate standards for countermeasures. To complete the risk management process for physical security of the data center facility, agency CIOs must work in coordination with other senior officials for security and facilities management within their agency.

Source: GAO analysis based on OMB Memorandum M-25-03. | GAO-27-108971

[a]We did not assess agencies against implementing data center maintenance practices that minimize planned downtime for hosted information systems and following modern software development practices to reduce impacts of data center downtime. This is because OMB's guidance did not specifically require agencies to do so. For example, the guidance notes that the agencies should implement data center maintenance practices that minimize planned downtime for hosted information systems where feasible and cost-effective. Additionally, guidance for following modern software development practices is broad and lacks measurable criteria to evaluate.

We requested relevant data center documentation from all 21 agencies and analyzed the documentation, including policies, procedures, and risk management and security plans, from the agencies that provided it. In some cases, the agencies did not have the requested information. We also obtained and analyzed responses from each of the 21 agencies to our semi-structured questions describing each agency's number of data

centers and efforts to incorporate OMB's requirements into their data centers. We then collected and compared agency documentation and responses to the requirements outlined in OMB Memorandum M-25-03. We supplemented our analysis with interviews or written communication with relevant agency officials to discuss the agencies' progress toward addressing these requirements, as appropriate. We also provided the results of our analysis of agency documentation to officials to corroborate our findings, collected additional evidence, and identified causes for any gaps in agencies' incorporation of the requirements. We then determined whether the evidence provided by the agencies addressed the evaluation criteria for each requirement. To determine an overall rating for each of the five requirements, we summarized the results of our assessments as:

- fully addressed—the agency fully addressed all of the requirement's evaluation criteria;
- partially addressed—the agency fully or partially addressed some, but not all, of the requirement's evaluation criteria; and
- not addressed—the agency did not address any of the requirement's evaluation criteria

Additionally, in our assessment we noted where the requirement did not apply to the agency because it reported having no new data centers, and because OMB did not specifically require agencies to apply the requirement to existing data centers.

To assess the reliability of data agencies provided from their data center inventories or other systems, we reviewed the documentation (e.g., spreadsheets and screenshots) related to the number of data centers for obvious issues and for completeness. We also interviewed agency officials and reviewed each agency's responses to questions about efforts to ensure that the data were accurate and complete. We determined that the agencies' data were sufficiently reliable for the purposes of this report.

We conducted this performance audit from February 2026 to November 2026 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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Appendix II: Detailed Assessment of Agencies' Incorporation of OMB's Data Center Requirements

This appendix contains detailed assessments of the extent to which the 21 federal agencies with new or existing data centers incorporated the Office of Management and Budget's (OMB) five acquisition and operational requirements into their data centers.[1]

Department of Agriculture

Table 5: Extent to Which Department of Agriculture Addressed the Five Office of Management and Budget Acquisition and Operational Data Center Requirements, as of August 2026

Requirement	Assessment	Summary of assessment
Make key data center decisions at the agency level	Partially addressed	Agriculture officials stated that the agency's Chief Information Officer (CIO) has overall responsibility for data center acquisition decision-making and operational management. However, the agency did not demonstrate that the requiring office and relevant procurement official consulted with the CIO throughout the process of procuring a new data center or making substantial changes to an existing one. Additionally, the agency did not demonstrate how it determined it was cost-effective and met agency mission needs to build a new data center rather than use commercial co-location services.
Monitor data center operations	Partially addressed	Agriculture's *System and Organization Controls for Service Organizations* report has controls for monitoring its new contractor-operated data center, including the use of automated tools, such as the Data Center Infrastructure Management (DCIM) system. Agriculture officials also stated that the agency uses these automated tools to monitor its data center operations, such as electrical consumption. However, it did not provide supporting documentation showing that it was using these tools to monitor operations for its one reported new data center.
Incorporate energy and water usage into decision-making	Partially addressed	Agriculture relies on the *System and Organization Controls for Service Organizations* report for its contractor-operated data center, which provides independent assurance over controls governing the contractor's use of the DCIM system to facilitate the exchange and analysis of data from energy; lightning; fire safety; and heating, ventilation, and air conditioning systems. Agriculture officials also stated that the agency utilizes DCIM tools for monitoring energy usage in agency-operated data centers and incorporates data into decision-making. However, no documentation was provided to demonstrate that while designing the new data center, the agency arranged for an assessment by specialists certified in data center energy efficiency.

[1]The Department of Education, the General Services Administration, and U.S. Agency for International Development did not report any data centers and thus were not included in our assessment.

Requirement	Assessment	Summary of assessment
Meet mission availability requirements	Partially addressed	Agriculture relies on the *System and Organization Controls for Service Organizations* report for its contractor-operated data center, which provides independent assurance over controls governing system availability, including using a business impact analysis. Additionally, the agency's risk analysis report identifies and evaluates system availability risks for its agency-operated data center. According to Agriculture officials, the agency operates under 99.9 percent uptime service level agreements supported by business impact analyses, annual disaster recovery testing with traffic being directed to a secondary site, redundant power infrastructure, backup generators, scheduled maintenance windows, and ongoing monitoring of uptime and power usage effectiveness. However, the agency did not demonstrate that it had an internal control process for managing risks to data center availability that used the results of a business impact analysis to set minimum requirements for each data center.
Meet information and physical security requirements	Partially addressed	Agriculture officials stated that its data centers comply with key requirements and are subject to annual monitoring and independent review. Specifically, Agriculture's *System and Organization Controls for Service Organizations* report states that its contractor-operated data center includes the Federal Information Security Modernization Act and National Institute of Standards and Technology controls for physical and information security. However, for both its new data center and its existing data center, the agency did not provide documentation to demonstrate that the CIO works in coordination with other senior officials for security and facilities management within their agency to complete the Interagency Security Committee risk management process.

Fully addressed: The agency fully addressed all of the requirement's evaluation criteria; Partially addressed: The agency fully or partially addressed some, but not all of the requirement's evaluation criteria; Not addressed: The agency did not address any of the requirement's evaluation criteria.

Source: GAO analysis of Department of Agriculture documentation. | GAO-27-108971

Department of Commerce

Table 6: Extent to Which Department of Commerce Addressed the Five Office of Management and Budget Acquisition and Operational Data Center Requirements, as of August 2026

Requirement	Assessment	Summary of assessment
Make key data center decisions at the agency level	Partially addressed	Commerce officials stated that the agency's component-level Chief Information Officers (CIO) are responsible for operational management and oversight of their respective data centers. These officials stated that the agency is developing a data center policy memorandum that would establish the agency CIO as the central authority for all data center acquisitions and operational modifications. Officials stated that the memorandum would require mandatory Office of the CIO consultation and documented cost-effectiveness analyses, including assessments of commercial co-location options, before approving new data center construction or major upgrades.[a]
Monitor data center operations	Partially addressed	While Commerce has draft memorandums that describe three of its components' approaches to implementing monitoring capabilities for new and existing data centers, agency officials stated that the agency is also developing a data center policy memorandum that would require the implementation of automated monitoring tools, including Data Center Infrastructure Management systems, and establish agencywide minimum monitoring standards for both new and existing data centers.[a]

Requirement	Assessment	Summary of assessment
Incorporate energy and water usage into decision-making	Partially addressed	Commerce officials stated that the agency is developing a data center policy memorandum that would require routine resource evaluations of data center consumption against federal metrics, require certified energy efficiency specialist assessments during planning and design phases, and formalize coordination with the agency's Chief Sustainability Officer and facilities management officials.[a]
Meet mission availability requirements	Partially addressed	Commerce's *Enterprise Services Center Service Level Agreement* provides expectations for mission availability, including system availability metrics and disaster recovery data center services. Additionally, Commerce officials stated that each operating unit includes contractual service level agreement provisions related to data center availability and monthly reviews are regularly performed to confirm acceptable quality levels. Officials also stated that the agency is developing a data center policy memorandum that would establish a centralized internal control process using business impact analyses to define standardized uptime objectives, disaster recovery requirements, and acceptable downtime tolerances for hosted systems.[a]
Meet information and physical security requirements	Partially addressed	Commerce's *Enterprise Cybersecurity Policy* and *Security and Privacy Assessment and Authorization* documentation establish agencywide cybersecurity requirements and processes for implementing, assessing, authorizing, and continuously monitoring security controls to protect information systems and support compliance with federal information and physical security requirements. Additionally, Commerce officials stated that the agency is developing a data center policy memorandum that would formalize agencywide compliance with the Federal Information Security Modernization Act, as well as National Institute of Standards and Technology and Interagency Security Committee risk management processes by requiring documented coordination between the agency CIO, security leadership, and facilities management officials.[a]

Fully addressed: The agency fully addressed all of the requirement's evaluation criteria; Partially addressed: The agency fully or partially addressed some, but not all of the requirement's evaluation criteria; Not addressed: The agency did not address any of the requirement's evaluation criteria.

Source: GAO analysis of Department of Commerce documentation. | GAO-27-108971

[a]On October 16, 2026, while the report was at the agency for comment, the department finalized its data center policy to address compliance gaps and optimization, and strengthen alignment with OMB's requirements, among other things. According to the policy, operating units and offices are required to implement the five OMB requirements, including the adoption of automated monitoring tools, within 90 business days.

Department of Defense

Table 7: Extent to Which Department of Defense (DOD) Addressed the Five Office of Management and Budget Acquisition and Operational Data Center Requirements, as of August 2026

Requirement	Assessment	Summary of assessment
Make key data center decisions at the agency level	Fully addressed	According to the *DOD Data Center Optimization Initiative* memorandum, and Section 2867 of the National Defense Authorization Act for Fiscal Year 2012, components are required to obtain Chief Information Officer (CIO) or designee approval prior to obligating funds for data centers or related technologies. The memorandum stated that DOD components use the IT Procurement Assessment Tool to support compliance with the agency's data center procurement approval process and to collect information needed to report on the amount spent on data centers.

Requirement	Assessment	Summary of assessment
		DOD reported that the number of new data centers was to be determined. Therefore, we did not assess whether the requiring office and the relevant procurement official consult with the agency's CIO throughout the process of procuring a new data center or making substantial changes to an existing one. Also, we did not assess whether the agency uses commercial co-location services rather than building new data centers to the extent that it is cost-effective and meets agency mission needs.
Monitor data center operations	Fully addressed	For its existing data centers, according to the *DOD Data Center Optimization Initiative* memorandum, the Data Center Infrastructure Management system is the agency's authoritative database for data center inventory reporting. It captures the current disposition of data center assets to include the type, location, size, and total physical and virtual server counts. DOD reported that the number of new data centers was to be determined. Therefore, we did not assess whether the agency incorporated automated tools into the management of all new data centers.
Incorporate energy and water usage into decision-making	—	DOD reported that the number of new data centers was to be determined. Therefore, we did not assess whether the agency evaluated data centers against resource consumption metrics and best practices when making decisions. DOD officials stated that the agency has incorporated sustainable energy sources and efficiency metrics into its decisions to maintain, upgrade or build new data centers. For existing data centers, these officials stated that its Data Center Reference Architecture ensures that its data centers deliver DOD information technology (IT) services in a manner optimized for performance and efficiency.
Meet mission availability requirements	Partially addressed	DOD officials stated that the CIO has integrated standards into its enterprise-wide Mission Network-as-a-Service framework, Data Center Reference Architecture, and cybersecurity policy to ensure that all data centers meet uptime and resiliency benchmarks required for multi-domain operations. However, it has not demonstrated that the agency used the results of a business impact analysis to set minimum availability requirements for each data center.
Meet information and physical security requirements	Partially addressed	DOD officials stated that it has policies in place for meeting information and physical security requirements for its data centers. However, for both new and existing data centers, the agency did not provide documentation to demonstrate that the CIO works in coordination with other senior officials for security and facilities management within their agency to complete the Interagency Security Committee risk management process.

Fully addressed: The agency fully addressed all of the requirement's evaluation criteria; Partially addressed: The agency fully or partially addressed some, but not all of the requirement's evaluation criteria; Not addressed: The agency did not address any of the requirement's evaluation criteria; — = The requirement did not apply to the agency as it reported it had no new data centers and because the Office of Management and Budget did not specifically require agencies to apply the requirement to existing data centers.

Source: GAO analysis of Department of Defense documentation. | GAO-27-108971

Department of Energy

Table 8: Extent to Which Department of Energy Addressed the Five Office of Management and Budget Acquisition and Operational Data Center Requirements, as of August 2026

Requirement	Assessment	Summary of assessment
Make key data center decisions at the agency level	Partially addressed	According to Energy officials, the agency has established an enterprise governance framework through which the Chief Information Officer (CIO) is actively engaged in the planning, budgeting, and execution of all information technology (IT) acquisitions. However, the agency has not sufficiently demonstrated that the requiring office and the relevant procurement official consult with the agency's CIO throughout the process of procuring a new data center or making substantial changes to an existing one. Furthermore, for the 29 percent of data centers reporting no CIO involvement, the agency stated that these facilities operate under a decentralized governance structure in which program offices, rather than the centralized CIO organization, oversee IT management.
Monitor data center operations	Partially addressed	According to Energy officials, the agency reported having one new data center, which is partially implementing the Data Center Infrastructure Management (DCIM) system or other automated tools to monitor facilities-related data. These officials noted that this new data center plans to fully implement DCIM systems once construction begins in July 2027. Energy officials also stated that approximately 90 percent of its existing data centers reported implementing automated tools, including the DCIM system, to monitor facilities-related data, such as electrical consumption.
Incorporate energy and water usage into decision-making	Partially addressed	According to Energy officials, while the agency reported having one new data center, it plans to obtain an assessment by specialists certified in data center energy efficiency once construction begins in July 2027. However, no documentation about these plans was provided. Officials also stated that for its existing data centers, approximately 88 percent reported fully or partially conducting energy and water assessments in coordination with the agency's Chief Sustainability Officer and facilities management representatives on a regular basis.
Meet mission availability requirements	Partially addressed	According to Energy officials, approximately 91 percent of data centers reported fully or partially implementing internal control processes to manage data center availability risks. Energy officials stated that data centers reporting no implementation efforts cited key challenges, including resource and funding limitations. To address these gaps, the officials stated that many facilities are actively transitioning toward compliance by implementing cloud resiliency services, deploying automated monitoring tools, or establishing new IT risk management contracts.
Meet information and physical security requirements	Partially addressed	According to Energy officials, approximately 88 percent of data centers adhered to the Interagency Security Committee risk management process. Energy officials stated that about 11 percent reported partial implementation and stated that they have ongoing initiatives to complete implementation. Furthermore, the remaining 1 percent of data centers reported managing physical security through other frameworks or incorporating Interagency Security Committee guidance into the design phase of new facilities.

Fully addressed: The agency fully addressed all of the requirement's evaluation criteria; Partially addressed: The agency fully or partially addressed some, but not all of the requirement's evaluation criteria; Not addressed: The agency did not address any of the requirement's evaluation criteria.

Source: GAO analysis of Department of Energy documentation. | GAO-27-108971

Department of Health and Human Services

Table 9: Extent to Which Department of Health and Human Services (HHS) Addressed the Five Office of Management and Budget Acquisition and Operational Data Center Requirements, as of August 2026

Requirement	Assessment	Summary of assessment
Make key data center decisions at the agency level	Partially addressed	According to HHS officials, the Chief Information Officer (CIO), or its designated component's CIO, is responsible for data center acquisition decision-making and operational management. However, the agency did not demonstrate that the requiring office and relevant procurement official consult with the CIO throughout the process of procuring a new data center or making substantial changes to an existing one. Furthermore, the agency did not demonstrate how it determined it was cost-effective and met agency mission needs to build a new data center rather than using commercial co-location services.
Monitor data center operations	Partially addressed	HHS provided examples of how its components incorporate automated tools, such as the Data Center Infrastructure Management system, into the management of its data centers, including tools that monitor facilities-related data such as electrical consumption. However, only one component reported having new data centers, and the agency did not provide supporting documentation to demonstrate how it incorporates these tools into the management of the new data centers. Additionally, for its existing data centers, it did not provide supporting documentation demonstrating its use of such tools.
Incorporate energy and water usage into decision-making	Partially addressed	HHS officials stated that data center decisions are made at the component level for this requirement. For example, one component stated that it incorporates energy efficiency considerations into its data center infrastructure upgrades intended to improve efficiency and reduce energy consumption. However, the component with the new data centers did not provide documentation to demonstrate that while designing the new data centers, it had arranged for an assessment by certified data center energy efficiency specialists.
Meet mission availability requirements	Partially addressed	HHS officials stated that data center decisions are made at the component level for this requirement. While HHS provided documentation demonstrating that one of its components was meeting mission availability requirements, it did not do so for all its components. Specifically, it did not demonstrate that HHS had an internal control process for managing risks to data center availability that used the results of a business impact analysis to set minimum requirements for each data center.
Meet information and physical security requirements	Partially addressed	HHS officials stated that data center decisions are made at the component level for this requirement. However, for both new and existing data centers across the agency, it did not provide documentation to demonstrate that the HHS CIO works in coordination with other senior officials for security and facilities management within the agency to complete the Interagency Security Committee risk management process.

Fully addressed: The agency fully addressed all of the requirement's evaluation criteria; Partially addressed: The agency fully or partially addressed some, but not all of the requirement's evaluation criteria; Not addressed: The agency did not address any of the requirement's evaluation criteria.

Source: GAO analysis of Department of Health and Human Services documentation. | GAO-27-108971

Department of Homeland Security

Table 10: Extent to Which Department of Homeland Security (DHS) Addressed the Five Office of Management and Budget Acquisition and Operational Data Center Requirements, as of August 2026

Requirement	Assessment	Summary of assessment
Make key data center decisions at the agency level	Fully addressed	DHS's delegation document states that the DHS Chief Information Officer (CIO) has delegated authority for the approval, management, and oversight of the agency's resources, including data center investments. DHS reported that it has no new data centers. Therefore, we did not assess whether the requiring office and the relevant procurement official consult with the agency's CIO throughout the process of procuring a new data center or making substantial changes to an existing one. Also, we did not assess whether it uses commercial co-location services rather than building new data centers to the extent that it is cost-effective and meets agency mission needs.
Monitor data center operations	Fully addressed	For its existing data centers, the agency uses automated tools to monitor the operations of its data centers. Specifically, DHS's *Performance Work Statement for Data Center and Cloud Optimization Support Services* and *Quality Assurance Surveillance Plan* describe procedures and service level requirements for the agency's information technology infrastructure and systems, including the use of automated monitoring capabilities. DHS reported that it has no new data centers. Therefore, we did not assess whether the agency incorporated automated tools into the management of all new data centers.
Incorporate energy and water usage into decision-making	—	DHS reported that it has no new data centers. Therefore, we did not assess whether the agency evaluated data centers against resource consumption metrics and best practices when making decisions.
Meet mission availability requirements	Partially addressed	The agency has established internal control processes to manage risks to availability in its Concept of Operations and Standard Operating Procedure documentation. Additionally, its *Performance Work Statement for Data Center and Cloud Optimization Support Services* and risk management implementation plan and guide describe how availability requirements are managed for its data center and risk management process. However, these documents did not demonstrate that the agency used the results of a business impact analysis to set minimum availability requirements for each data center.
Meet information and physical security requirements	Fully addressed	The agency's *Instruction Manual 121-01-010-01 Physical Security* describes how the agency meets physical security requirements, including how it uses an Interagency Security Committee risk management process and communicates with others, such as the Chief Security Officer, Facility Security Committee, and physical security officials, to complete the process for physical security of the data center facilities. Additionally, its security and privacy plan describes controls on securing information and physical facilities of the data centers. Furthermore, DHS's CIO works in coordination with other senior officials for security and facilities management within their agency to complete the Interagency Security Committee risk management process.

Fully addressed: The agency fully addressed all of the requirement's evaluation criteria; Partially addressed: The agency fully or partially addressed some, but not all of the requirement's evaluation criteria; Not addressed: The agency did not address any of the requirement's evaluation criteria; — = The requirement did not apply to the agency as it reported it had no new data centers and because the Office of Management and Budget did not specifically require agencies to apply the requirement to existing data centers.

Source: GAO analysis of Department of Homeland Security documentation. | GAO-27-108971

Department of Housing and Urban Development

Table 11: Extent to Which Department of Housing and Urban Development (HUD) Addressed the Five Office of Management and Budget Acquisition and Operational Data Center Requirements, as of August 2026

Requirement	Assessment	Summary of assessment
Make key data center decisions at the agency level	Partially addressed	HUD reported that the agency has centralized data center acquisition decision-making and operational management under its Chief Information Officer (CIO) but did not demonstrate how the CIO is making key data center decisions. HUD reported that it has no new data centers. Therefore, we did not assess whether the requiring office and the relevant procurement official consult with the agency's CIO throughout the process of procuring a new data center or making substantial changes to an existing one. Also, we did not assess whether it uses commercial co-location services rather than building new data centers to the extent that it is cost-effective and meets agency mission needs.
Monitor data center operations	Fully addressed	For its existing data centers, HUD uses automated monitoring tools such as the Data Center Infrastructure Management system. HUD reported that it has no new data centers. Therefore, we did not assess whether the agency incorporated automated tools into the management of all new data centers.
Incorporate energy and water usage into decision-making	—	HUD reported that it has no new data centers. Therefore, we did not assess whether the agency evaluated data centers against resource consumption metrics and best practices when making decisions.
Meet mission availability requirements	Partially addressed	HUD officials stated that for all applicable data centers, the agency has implemented risk avoidance and mitigation controls to meet availability targets. However, the agency did not demonstrate that it had an internal control process for managing risks to data center availability that used the results of a business impact analysis to set minimum requirements for each data center.
Meet information and physical security requirements	Partially addressed	HUD officials stated that the agency inherits Federal Information Security Modernization Act compliance and National Institute of Standards and Technology security controls from hosting providers to meet security requirements and has adhered to Interagency Security Committee risk management processes related to physical security of all covered data centers. HUD also provided documentation that establishes the standards, guidelines, and procedures relating to the operational security and the physical protection of the facility and assets. However, for both new and existing data centers, the document provided did not state that the CIO works in coordination with other senior officials for security and facilities management within their agency to complete the Interagency Security Committee risk management process.

Fully addressed: The agency fully addressed all of the requirement's evaluation criteria; Partially addressed: The agency fully or partially addressed some, but not all of the requirement's evaluation criteria; Not addressed: The agency did not address any of the requirement's evaluation criteria; — = The requirement did not apply to the agency as it reported it had no new data centers and because the Office of Management and Budget did not specifically require agencies to apply the requirement to existing data centers.

Source: GAO analysis of Department of Housing and Urban Development documentation. | GAO-27-108971

Department of the Interior

Table 12: Extent to Which Department of the Interior Addressed the Five Office of Management and Budget Acquisition and Operational Data Center Requirements, as of August 2026

Requirement	Assessment	Summary of assessment
Make key data center decisions at the agency level	Fully addressed	According to Interior's *Departmental Manual Part 112 Chapter 24* and *Hosting Services Policy* documents, data center acquisition decision-making and operational management are centralized with the Chief Information Officer (CIO), and the requiring office and relevant procurement official consult with the CIO throughout the budget and acquisition process. While Interior does not have any new data centers, the policy document directs the use of commercial services as the preferred first option, prior to consideration of agency-built data centers.
Monitor data center operations	Partially addressed	For its existing data centers, Interior officials stated that the agency has partially implemented automated monitoring tools and plans to expand deployment to remaining data centers to the extent that it is cost effective. Interior reported that it has no new data centers. Therefore, we did not assess whether the agency incorporated automated tools into the management of all new data centers.
Incorporate energy and water usage into decision-making	—	Interior reported that it has no new data centers. Therefore, we did not assess whether the agency evaluated data centers against resource consumption metrics and best practices when making decisions. Interior's key mission facility policy codifies the requirement to implement automated energy and water metering for data centers larger than 1,000 square feet, but not all data centers.
Meet mission availability requirements	Partially addressed	Interior's *Data Center Classification, Reporting, and Key Mission Facility Requirements* policy stated that for its new data centers, the agency must meet minimum high standards for requirements, including availability. Also, Interior's *Hosting Services Policy* states that the agency's bureau or Office Associate CIOs must submit a request for approval to make a financial decision related to a data center, including a description of how the center will enable the hosted information or information systems to meet appropriate availability and uptime requirements. According to Interior officials, individual data center managers are monitoring data center availability, without centralized enterprise tracking or reporting. However, Interior did not sufficiently demonstrate that the agency had an internal control process for managing risks to data center availability that used the results of a business impact analysis to set minimum requirements for each data center.
Meet information and physical security requirements	Partially addressed	According to Interior officials, physical access to data center facilities is controlled and the Office of the CIO manages logical access to systems, while data center managers are responsible for facility access controls and building security systems. Interior's *Hosting Services Policy* requires the agency to submit a request for approval to make a financial decision related to a data center, including a statement of assurance that the data center will meet the appropriate information and physical security requirements. However, for both new and existing data centers, the document provided did not state that the CIO works in coordination with other senior officials for security and facilities management within their agency to complete the Interagency Security Committee risk management process.

Fully addressed: The agency fully addressed all of the requirement's evaluation criteria; Partially addressed: The agency fully or partially addressed some, but not all of the requirement's evaluation criteria; Not addressed: The agency did not address any of the requirement's evaluation criteria; — = The requirement did not apply to the agency as it reported it had no new data centers and because the Office of Management and Budget did not specifically require agencies to apply the requirement to existing data centers.

Source: GAO analysis of Department of the Interior documentation. | GAO-27-108971

Department of Justice

Table 13: Extent to Which Department of Justice Addressed the Five Office of Management and Budget Acquisition and Operational Data Center Requirements, as of August 2026

Requirement	Assessment	Summary of assessment
Make key data center decisions at the agency level	Fully addressed	Justice's *Policy Statement 0900.01* and *Data Center Actions Information Technology Action* memorandum establish Chief Information Officer (CIO) oversight of information technology (IT) and data center investments, including review and approval of applicable component acquisition plans and data center proposals. Additionally, the memorandum describes a process to request Justice's CIO's approval in advance of any related task initiation or funding. It provides a mechanism for CIO involvement in acquisition decision-making consistent with the Office of Management and Budget's expectation that the requiring office and relevant procurement official consult with the CIO throughout the process of procuring a new data center or making substantial changes to an existing one. Justice reported that it has no new data centers. Therefore, we did not assess whether it uses commercial co-location services rather than building new data centers to the extent that it is cost-effective and meets agency mission needs.
Monitor data center operations	Fully addressed	Justice's *Data Center Actions Information Technology Action* memorandum states that the agency must implement the Data Center Infrastructure Management system for new and existing data centers and when making substantial upgrades to existing data centers. Justice reported that it has no new data centers. Therefore, we did not assess whether the agency incorporated automated tools into the management of all new data centers.
Incorporate energy and water usage into decision-making	—	Justice reported that it has no new data centers. Therefore, we did not assess whether the agency evaluated data centers against resource consumption metrics and best practices when making decisions. Justice's *Data Center Actions Information Technology Action* memorandum indicates that if a component plans to procure a new data center or if the component is planning to make substantial upgrades to an existing data center, then the data center is subject to additional compliance requirements, including completing a resource (e.g., energy, water) efficiency assessment.
Meet mission availability requirements	Fully addressed	Justice's *Cybersecurity Program Order* and *Information System Contingency Plan* require components to define system availability requirements including using the results of a business impact analysis, implementing contingency planning, and managing risks to ensure the availability and continuity of mission-critical information systems, which include data centers. Additionally, according to Justice's *Data Center Actions Information Technology Action* memorandum, component CIOs operating data centers must establish a target availability of 99.8 percent for each component-operated data center and report actual availability for the data center on a semi-annual basis via a data call. Risks affecting each data center's availability must be identified and mitigated in accordance with Justice's *Information Systems Contingency Planning Guide*.

Requirement	Assessment	Summary of assessment
Meet information and physical security requirements	Partially addressed	According to Justice's *Data Center Actions Information Technology Action* memorandum, component CIOs must ensure compliance with the agency's cybersecurity policy and the Interagency Security Committee risk management process related to the physical security for each component-operated data center. Justice's *IT Order 0904 Cybersecurity Program* states the requirements for managing information security, including National Institute of Standards and Technology and Financial Information Security Modernization Act guidance. However, for both new and existing data centers, the documents provided did not state that the CIO works in coordination with other senior officials for security and facilities management within their agency to complete the Interagency Security Committee risk management process.

Fully addressed: The agency fully addressed all of the requirement's evaluation criteria; Partially addressed: The agency fully or partially addressed some, but not all of the requirement's evaluation criteria; Not addressed: The agency did not address any of the requirement's evaluation criteria; — = The requirement did not apply to the agency as it reported it had no new data centers and because the Office of Management and Budget did not specifically require agencies to apply the requirement to existing data centers.

Source: GAO analysis of Department of Justice documentation. | GAO-27-108971

Department of Labor

Table 14: Extent to Which Department of Labor Addressed the Five Office of Management and Budget Acquisition and Operational Data Center Requirements, as of August 2026

Requirement	Assessment	Summary of assessment
Make key data center decisions at the agency level	Fully addressed	Labor's data center acquisition and operational decisions are centralized under the Chief Information Officer (CIO). While Labor did not report any new data centers, it stated that the agency uses commercial solutions through the Equinix co-location facility and expanded use of cloud services. We did not assess whether the requiring office and the relevant procurement official consult with the agency's CIO throughout the process of procuring a new data center or making substantial changes to an existing one.
Monitor data center operations	Fully addressed	For its existing data centers, Labor uses a Data Center Infrastructure Management tool to monitor power, environmental conditions, and mechanical and electrical systems in real time across its co-located data center footprint. Labor reported that it has no new data centers. Therefore, we did not assess whether the agency incorporated automated tools into the management of all new data centers.
Incorporate energy and water usage into decision-making	—	Labor reported that it has no new data centers. Therefore, we did not assess whether the agency evaluated data centers against resource consumption metrics and best practices when making decisions. For its existing data centers, the agency stated that it relies on an energy efficiency program at its facility to monitor power usage effectiveness, cooling, and electricity use and support planning for its co-located data center.
Meet mission availability requirements	Partially addressed	Labor stated that it ensures mission availability through a combination of internal policy, system-level monitoring, and infrastructure design. Additionally, Labor provided examples of independent assessments on information related to mission availability. However, these documents did not sufficiently demonstrate that the agency had an internal control process for managing risks to data center availability that used the results of a business impact analysis to set minimum requirements for each data center.

Requirement	Assessment	Summary of assessment
Meet information and physical security requirements	Partially addressed	Labor stated that hosted systems follow security standards with ongoing authorization and continuous monitoring. While the agency provided documentation that its facility has physical security controls and that it coordinates with security and facilities staff under the Interagency Security Committee process, the documentation does not specify that the CIO works in coordination with these officials in doing so.

Fully addressed: The agency fully addressed all of the requirement's evaluation criteria; Partially addressed: The agency fully or partially addressed some, but not all of the requirement's evaluation criteria; Not addressed: The agency did not address any of the requirement's evaluation criteria; — = The requirement did not apply to the agency as it reported it had no new data centers and because the Office of Management and Budget did not specifically require agencies to apply the requirement to existing data centers.

Source: GAO analysis of Department of Labor documentation. | GAO-27-108971

Department of State

Table 15: Extent to Which Department of State Addressed the Five Office of Management and Budget Acquisition and Operational Data Center Requirements, as of August 2026

Requirement	Assessment	Summary of assessment
Make key data center decisions at the agency level	Fully addressed	According to State's Information Technology Acquisition policies, the department's Chief Information Officer (CIO) is responsible for oversight of all information technology procurement including data center decisions. State reported that it has no new data centers. Therefore, we did not assess whether the requiring office and the relevant procurement official consult with the agency's CIO throughout the process of procuring a new data center or making substantial changes to an existing one. Also, we did not assess whether it uses commercial co-location services rather than building new data centers to the extent that it is cost-effective and meets agency mission needs.
Monitor data center operations	Fully addressed	For its existing data centers, State has deployed a Data Center Infrastructure Management platform to automate monitoring of its data centers. State reported that it has no new data centers. Therefore, we did not assess whether the agency incorporated automated tools into the management of all new data centers.
Incorporate energy and water usage into decision-making	—	State officials stated that there are no plans to build new data centers or make substantial upgrades. Therefore, we did not assess whether the agency evaluated data centers against resource consumption metrics and best practices when making decisions. For its existing data centers, agency officials stated that there is coordination with data center facilities to obtain data necessary for comprehensive resource usage monitoring.
Meet mission availability requirements	Partially addressed	State officials stated that its data centers meet availability requirements, and the agency follows standards to minimize planned downtime to meet mission availability requirements and has adopted modern software development practices, such as cloud services. According to State officials, business impact analyses are conducted as part of the authorization to operate process. The agency also described how it conducts business impact analysis as part of its authorization to operate process, and identified metrics, including maximum tolerable downtime and recovery time objectives for its enterprise data centers. However, it did not sufficiently demonstrate that the agency had an internal control process for managing risks to data center availability including using the results of a business impact analysis to set minimum availability requirements for all its data centers that will meet the availability needs of its hosted information and information systems.

Requirement	Assessment	Summary of assessment
Meet information and physical security requirements	Fully addressed	State officials stated that its enterprise data centers meet all associated security standards. State's Authority to Operate approvals demonstrate that the Data Center Infrastructure Management platform and Enterprise Data Center system were reviewed and authorized under the agency's security process. State officials stated that its Bureau of Diplomatic Security conducts physical security inspections and risk assessment of the agency's domestic data centers in coordination with the designated official responsible for each facility, who reports to the CIO. State's physical security risk assessment documentation demonstrates this process.

Fully addressed: The agency fully addressed all of the requirement's evaluation criteria; Partially addressed: The agency fully or partially addressed some, but not all of the requirement's evaluation criteria; Not addressed: The agency did not address any of the requirement's evaluation criteria; — = The requirement did not apply to the agency as it reported it had no new data centers and because the Office of Management and Budget did not specifically require agencies to apply the requirement to existing data centers.

Source: GAO analysis of Department of State documentation. | GAO-27-108971

Department of Transportation

Table 16: Extent to Which Department of Transportation Addressed the Five Office of Management and Budget Acquisition and Operational Data Center Requirements, as of August 2026

Requirement	Assessment	Summary of assessment
Make key data center decisions at the agency level	Fully addressed	According to Transportation officials, all data centers are monitored and managed within the Office of the Chief and Digital Information Officer with delegated authority to the Federal Aviation Administration (FAA) as appropriate. Specifically, FAA provides guidance with *Order 1100.171B*, which states that FAA's Chief Information Officer (CIO) manages and maintains its data centers. Transportation reported that it has no new data centers. Therefore, we did not assess whether the requiring office and the relevant procurement official consult with the agency's CIO throughout the process of procuring a new data center or making substantial changes to an existing one. Also, we did not assess whether it uses commercial co-location services rather than building new data centers to the extent that it is cost-effective and meets agency mission needs.
Monitor data center operations	Fully addressed	For its existing data centers, Transportation monitors its data centers using its Data Center Infrastructure Management tool. Transportation reported that it has no new data centers. Therefore, we did not assess whether the agency incorporated automated tools into the management of all new data centers.
Incorporate energy and water usage into decision-making	—	Transportation reported that it has no new data centers. Therefore, we did not assess whether the agency evaluated data centers against resource consumption metrics and best practices when making decisions. For its existing data centers, Transportation officials stated that it monitors environmental health for its data centers, and it delegates authority to one of its components, FAA, as appropriate.
Meet mission availability requirements	Partially addressed	While one of Transportation's components, FAA, demonstrated meeting mission availability requirements for its data centers, the agency did not provide documentation of doing so for its agency-level data centers. *FAA Order 1100.171B* states that the Operations and Maintenance Branch is responsible for configuring the operating system environment for system disaster recovery solutions, which supports system availability, and FAA developed a business impact analysis. However, Transportation did not demonstrate that it used the results of a business impact analysis to set minimum availability requirements for each data center.

Requirement	Assessment	Summary of assessment
Meet information and physical security requirements	Partially addressed	Transportation officials stated that its data centers are monitored for physical, environmental, network, and hardware health, with alerts when thresholds are exceeded. The agency's *Data Center Standards* document defines the standards for material, infrastructure, design, installation, and certification with respect to structured data centers at the agency's facilities. However, this document does not describe how the Transportation CIO works in coordination with other senior officials for security and facilities management within their agency to complete the Interagency Security Committee risk management process.

Fully addressed: The agency fully addressed all of the requirement's evaluation criteria; Partially addressed: The agency fully or partially addressed some, but not all of the requirement's evaluation criteria; Not addressed: The agency did not address any of the requirement's evaluation criteria; — = The requirement did not apply to the agency as it reported it had no new data centers and because the Office of Management and Budget did not specifically require agencies to apply the requirement to existing data centers.

Source: GAO analysis of Department of Transportation documentation. | GAO-27-108971

Department of the Treasury

Table 17: Extent to Which Department of the Treasury Addressed the Five Office of Management and Budget Acquisition and Operational Data Center Requirements, as of August 2026

Requirement	Assessment	Summary of assessment
Make key data center decisions at the agency level	Fully addressed	According to the agency's draft *Treasury Common Services Center (TCSC) IT Service Line Roles, Responsibilities, and Activities* document, data center management is assigned to the TCSC and associated bureaus and offices. Additionally, according to the agency's *Treasury Order 102-10*, the agency Chief Information Officer (CIO) is responsible for planning, programming, budgeting, and execution of information technology (IT) including data centers. Treasury reported that it has no new data centers. Therefore, we did not assess whether the requiring office and the relevant procurement official consult with the agency's CIO throughout the process of procuring a new data center or making substantial changes to an existing one. Also, we did not assess whether the agency uses commercial co-location services rather than building new data centers to the extent that it is cost-effective and meets agency mission needs.
Monitor data center operations	Not addressed	For its existing data centers, the agency did not provide related supporting documentation demonstrating its use of automated tools to monitor the operations of its data centers. Treasury reported that it has no new data centers. Therefore, we did not assess whether the agency incorporated automated tools into the management of all new data centers.
Incorporate energy and water usage into decision-making	—	Treasury reported that it has no new data centers. Therefore, we did not assess whether the agency evaluated data centers against resource consumption metrics and best practices when making decisions. For its existing data centers, Treasury officials stated that its *2024-2027 Climate Adaptation Plan* discusses, among other things, facility resilience, energy efficiency, and modernization.

Requirement	Assessment	Summary of assessment
Meet mission availability requirements	Partially addressed	Treasury officials stated that data center availability and continuity are managed through bureau-operated facilities with enterprise-level oversight and resilience planning. Treasury's *Fiscal Year 2025 Federal Information Security Modernization Act Evaluation Report*, *2024-2027 Climate Adaptation Plan*, and *TCSC Roles and Responsibilities* describe incident response, cloud adoption, and operational resilience activities. According to Treasury officials, its existing data centers continue to operate under established business impact analyses. However, the agency has not provided documentation to support that it used the results of a business impact analysis to set minimum availability requirements for each data center.
Meet information and physical security requirements	Fully addressed	Treasury officials stated that the agency uses a shared model aligned with Federal Information Security Management Act, National Institute of Standards and Technology, and Interagency Security Committee standards to meet federal information security and physical security requirements. It also provided documentation that describes the agency's security governance, access control, and data center operational security responsibilities. Additionally, the agency's security policies and plans delegate authority to the CIO over information systems and demonstrate that the CIO works in coordination with other senior officials for security and facilities management within their agency.

Fully addressed: The agency fully addressed all of the requirement's evaluation criteria; Partially addressed: The agency fully or partially addressed some, but not all of the requirement's evaluation criteria; Not addressed: The agency did not address any of the requirement's evaluation criteria; — = The requirement did not apply to the agency as it reported it had no new data centers and because the Office of Management and Budget did not specifically require agencies to apply the requirement to existing data centers.

Source: GAO analysis of Department of the Treasury documentation. | GAO-27-108971

Department of Veterans Affairs

Table 18: Extent to Which Department of Veterans Affairs (VA) Addressed the Five Office of Management and Budget Acquisition and Operational Data Center Requirements, as of August 2026

Requirement	Assessment	Summary of assessment
Make key data center decisions at the agency level	Partially addressed	VA officials stated that the agency has initiated efforts to develop a directive that would require all sites to implement a centralized enterprise approach and expects to finalize the directive by the third quarter of fiscal year 2027. VA reported that it has no new data centers. Therefore, we did not assess whether the requiring office and the relevant procurement official consult with the agency's Chief Information Officer (CIO) throughout the process of procuring a new data center or making substantial changes to an existing one. Also, we did not assess whether it uses commercial co-location services rather than building new data centers to the extent that it is cost-effective and meets agency mission needs.
Monitor data center operations	Partially addressed	For its existing data centers, VA officials stated that the agency uses energy and asset optimizer tools, which enable real-time monitoring of data center infrastructure and management of technology assets within data centers for efficient capacity management. However, the agency did not provide supporting documentation demonstrating its use of such tools. VA reported that it has no new data centers. Therefore, we did not assess whether the agency incorporated automated tools into the management of all new data centers.

Requirement	Assessment	Summary of assessment
Incorporate energy and water usage into decision-making	—	VA reported that it has no new data centers. Therefore, we did not assess whether the agency evaluated data centers against resource consumption metrics and best practices when making decisions. For its existing data centers, VA officials stated that the agency is improving energy efficiency at enterprise data centers by employing hot and cold aisle containment systems and solar panels to enhance overall energy efficiency.
Meet mission availability requirements	Partially addressed	VA officials stated that the agency manages risk through a continuous authorization monitoring process which allows for the processing of risk management framework items including authorities to operate and plans of action and milestones. The officials also stated that its enterprise data centers are assessed through the standard security and risk management processes. While VA's *Directive 6500* and *Handbook 6500* govern the agency's foundational cybersecurity requirements, these documents did not describe using the results of a business impact analysis to set minimum availability requirements for each data center.
Meet information and physical security requirements	Partially addressed	VA officials stated that all sites comply with Interagency Security Committee standards. VA provided a physical security manual and policy documentation to demonstrate the agency's physical security requirements. However, for both new and existing data centers, these documents did not state that the CIO or Office of Information and Technology works in coordination with other senior officials for security and facilities management within their agency to complete the Interagency Security Committee risk management process.

Fully addressed: The agency fully addressed all of the requirement's evaluation criteria; Partially addressed: The agency fully or partially addressed some, but not all of the requirement's evaluation criteria; Not addressed: The agency did not address any of the requirement's evaluation criteria; — = The requirement did not apply to the agency as it reported it had no new data centers and because the Office of Management and Budget did not specifically require agencies to apply the requirement to existing data centers.

Source: GAO analysis of Department of Veterans Affairs documentation. | GAO-27-108971

Environmental Protection Agency

Table 19: Extent to Which Environmental Protection Agency (EPA) Addressed the Five Office of Management and Budget Acquisition and Operational Data Center Requirements, as of August 2026

Requirement	Assessment	Summary of assessment
Make key data center decisions at the agency level	Partially addressed	EPA officials stated that key data center decisions are made at the agency level and that changes must be submitted through a change request by the supporting contractor or the federal point of contact and approved by the Chief Information Officer (CIO) prior to making any changes. However, supporting documentation of this was not provided. EPA reported that it has no new data centers. Therefore, we did not assess whether the requiring office and the relevant procurement official consult with the agency's CIO throughout the process of procuring a new data center or making substantial changes to an existing one. Also, we did not assess whether it uses commercial co-location services rather than building new data centers to the extent that it is cost-effective and meets agency mission needs.

Requirement	Assessment	Summary of assessment
Monitor data center operations	Fully addressed	For its existing data centers, EPA is using a Data Center Infrastructure Management system to monitor the operations of its data centers, including power consumption and heat produced. EPA reported that it has no new data centers. Therefore, we did not assess whether the agency incorporated automated tools into the management of all new data centers. EPA officials stated that the agency is transitioning to a new automated tool that would enhance data center monitoring and decision-making.
Incorporate energy and water usage into decision-making	—	EPA reported that it has no new data centers. Therefore, we did not assess whether the agency evaluated data centers against resource consumption metrics and best practices when making decisions. EPA officials stated that there is an internal agency action to baseline historical power and water utilization for the data centers.
Meet mission availability requirements	Partially addressed	EPA officials stated that data center customers maintain signed business impact statements and contingency plans that are updated annually. In addition, the agency officials also stated that EPA uses system security plans to identify and mitigate controls. However, it has not demonstrated that the agency used the results of a business impact analysis to set minimum availability requirements for each data center.
Meet information and physical security requirements	Partially addressed	EPA officials stated that physical security is handled through badge readers, gate access, approved access, and 24/7 monitoring by console operators. For information security, systems in the data center rely on continuous monitoring, including vulnerability scans, system security plans, annual contingency plan and incident response exercises, and annual audits. However, for both new and existing data centers, the agency did not provide documentation to demonstrate that the CIO works in coordination with other senior officials for security and facilities management within their agency to complete the Interagency Security Committee risk management process.

Fully addressed: The agency fully addressed all of the requirement's evaluation criteria; Partially addressed: The agency fully or partially addressed some, but not all of the requirement's evaluation criteria; Not addressed: The agency did not address any of the requirement's evaluation criteria; — = The requirement did not apply to the agency as it reported it had no new data centers and because the Office of Management and Budget did not specifically require agencies to apply the requirement to existing data centers.

Source: GAO analysis of Environmental Protection Agency documentation. | GAO-27-108971

National Aeronautics and Space Administration

Table 20: Extent to Which National Aeronautics and Space Administration (NASA) Addressed the Five Office of Management and Budget Acquisition and Operational Data Center Requirements, as of August 2026

Requirement	Assessment	Summary of assessment
Make key data center decisions at the agency level	Partially addressed	NASA officials stated that it is updating its information technology (IT) authorization process and real property data center facility decision-making process to include data center servers, storage, and Chief Information Officer (CIO) review, with completion planned for November 2026. NASA reported that it has no new data centers. Therefore, we did not assess whether the requiring office and the relevant procurement official consult with the agency's CIO throughout the process of procuring a new data center or making substantial changes to an existing one. Also, we did not assess whether it uses commercial co-location services rather than building new data centers to the extent that it is cost-effective and meets agency mission needs.

Requirement	Assessment	Summary of assessment
Monitor data center operations	Partially addressed	For its existing data centers, NASA stated that it uses Data Center Infrastructure Management systems and other tools to monitor data centers. Additionally, the NASA CIO has funded implementation of a standard enterprise Data Center Infrastructure Management solution with centralized monitoring capabilities. The agency expects to implement this solution in calendar year 2026, and a detailed project plan is currently being developed. NASA reported that it has no new data centers. Therefore, we did not assess whether the agency incorporated automated tools into the management of all new data centers. NASA officials did state that the agency plans to incorporate automated tools into the management of any new data centers approved in the future.
Incorporate energy and water usage into decision-making	—	NASA reported that it has no new data centers. Therefore, we did not assess whether the agency evaluated data centers against resource consumption metrics and best practices when making decisions. NASA officials stated that the agency's energy program manager is responsible for energy savings and sustainability improvements for new facility construction and major facility modifications. Officials also stated that NASA contracted with a third party to assess all agency data center facilities, including evaluations of energy efficiency, existing resource usage, and opportunities to improve efficiency.
Meet mission availability requirements	Partially addressed	NASA officials stated that data center availability is managed through system security plans and a risk based decision process, but not all requirements are currently met because of aging infrastructure and maintenance shortfalls. Specifically, officials stated that the agency is conducting a comprehensive review of assets and workloads to assess service level agreements and validate technical and operational availability requirements across its data centers, expected to be completed by the end of calendar year 2026. Officials further stated that the agency is implementing enterprise-wide standards for data center tiering and application criticality categories to improve availability management. Officials also stated that a centralized risk mitigation plan is being developed in conjunction with this analysis and is expected to be completed by November 2026.
Meet information and physical security requirements	Partially addressed	NASA officials said the agency meets most information security and data center physical security requirements, but some physical controls are still missing due to funding shortfalls. NASA's Data Center Optimization Strategy is intended to address these gaps, but it will require substantial funding and take multiple years.

Fully addressed: The agency fully addressed all of the requirement's evaluation criteria; Partially addressed: The agency fully or partially addressed some, but not all of the requirement's evaluation criteria; Not addressed: The agency did not address any of the requirement's evaluation criteria; — = The requirement did not apply to the agency as it reported it had no new data centers and because the Office of Management and Budget did not specifically require agencies to apply the requirement to existing data centers.

Source: GAO analysis of National Aeronautics and Space Administration documentation. | GAO-27-108971

National Science Foundation

Table 21: Extent to Which National Science Foundation (NSF) Addressed the Five Office of Management and Budget Acquisition and Operational Data Center Requirements, as of August 2026

Requirement	Assessment	Summary of assessment
Make key data center decisions at the agency level	Partially addressed	According to NSF officials, the agency makes key data center decisions through the Chief Information Officer (CIO), but no supporting documentation was provided. NSF reported that it has no new data centers. Therefore, we did not assess whether the requiring office and the relevant procurement official consult with the agency's CIO throughout the process of procuring a new data center or making substantial changes to an existing one. Also, we did not assess whether it uses commercial co-location services rather than building new data centers to the extent that it is cost-effective and meets agency mission needs.
Monitor data center operations	Partially addressed	For its existing data centers, according to NSF officials, the agency monitors data center operations 24/7 and utilizes automated monitoring capabilities. However, the agency did not provide supporting documentation demonstrating its use of such tools. NSF reported that it has no new data centers. Therefore, we did not assess whether the agency incorporated automated tools into the management of all new data centers.
Incorporate energy and water usage into decision-making	—	NSF reported that it has no new data centers. Therefore, we did not assess whether the agency evaluated data centers against resource consumption metrics and best practices when making decisions. NSF officials stated that if the agency does consider data center upgrades, it will plan to assess data center energy efficiency and resource usage in the design process. For its existing data centers, according to NSF officials, the agency has incorporated energy and water usage considerations into decision-making.
Meet mission availability requirements	Partially addressed	NSF officials stated that the agency has partially implemented an internal control process to evaluate data center availability. However, it did not demonstrate that the agency used the results of a business impact analysis to set minimum availability requirements for each data center.
Meet information and physical security requirements	Partially addressed	NSF officials stated that the agency has implemented appropriate information security and physical security protections for the agency's data center and associated systems. According to NSF officials, the agency implements Interagency Security Committee physical security. However, for both new and existing data centers, the agency did not provide documentation to demonstrate that the CIO works in coordination with other senior officials for security and facilities management within their agency to complete the Interagency Security Committee risk management process.

Fully addressed: The agency fully addressed all of the requirement's evaluation criteria; Partially addressed: The agency fully or partially addressed some, but not all of the requirement's evaluation criteria; Not addressed: The agency did not address any of the requirement's evaluation criteria; — = The requirement did not apply to the agency as it reported it had no new data centers and because the Office of Management and Budget did not specifically require agencies to apply the requirement to existing data centers.

Source: GAO analysis of National Science Foundation documentation. | GAO-27-108971

Nuclear Regulatory Commission

Table 22: Extent to Which Nuclear Regulatory Commission (NRC) Addressed the Five Office of Management and Budget Acquisition and Operational Data Center Requirements, as of August 2026

Requirement	Assessment	Summary of assessment
Make key data center decisions at the agency level	Fully addressed	NRC's *Management Directive 11.1* includes the Chief Information Officer's (CIO) role in acquisitions, including data centers. Additionally, NRC officials stated that data center management is delegated to the data center manager for tracking and reporting. The agency demonstrated that the requiring office and the relevant procurement official consult with the agency's CIO throughout the process of procuring a new data center or making substantial changes to an existing one. Furthermore, the agency provided evidence to demonstrate how it determined it was cost-effective and met agency mission needs to build a new data center rather than use commercial co-location services.
Monitor data center operations	Fully addressed	NRC's data center dashboard and the reports from the Data Center Infrastructure Management system demonstrate the agency's use of automated tools for monitoring data center operations for its new data centers, including tracking energy usage in its current data centers.
Incorporate energy and water usage into decision-making	Partially addressed	NRC provided documentation identifying a certified Data Center Energy Practitioner currently employed by NRC. This individual serves as the Administrative Contracting Officer's Representative for the Equinix co-location contracts and as the Office of the Chief Information Officer's technical advisor for all data center-related projects. Additionally, NRC described how it considered an existing data center's resource usage when making its design and selection decisions, but did not demonstrate how the agency reviewed and considered the assessment's recommendations in coordination with the agency's Chief Sustainability Officer and the agency's facilities management representatives when reviewing and considering the assessment recommendations.
Meet mission availability requirements	Partially addressed	NRC officials stated that mission-essential applications with high availability needs are being migrated to co-locations, cloud services, or other platforms that meet those requirements. In addition, the officials stated that NRC has procured equipment, completed modernizations, and developed migration plans, with all efforts expected to be completed by March 12, 2027.
Meet information and physical security requirements	Fully addressed	NRC's Security Cover Letter demonstrates that every security assessment for a facility, including data centers, is conducted to address physical security. Additionally, NRC's signed Authority to Operate letter documents information security assessments. For both new and existing data centers, the agency demonstrated that the CIO works in coordination with other senior officials for security and facilities management within their agency to complete the Interagency Security Committee risk management process.

Fully addressed: The agency fully addressed all of the requirement's evaluation criteria; Partially addressed: The agency fully or partially addressed some, but not all of the requirement's evaluation criteria; Not addressed: The agency did not address any of the requirement's evaluation criteria.

Source: GAO analysis of Nuclear Regulatory Commission documentation. | GAO-27-108971

Office of Personnel Management

Table 23: Extent to Which Office of Personnel Management (OPM) Addressed the Five Office of Management and Budget Acquisition and Operational Data Center Requirements, as of August 2026

Requirement	Assessment	Summary of assessment
Make key data center decisions at the agency level	Partially addressed	OPM officials stated that they have made key decisions regarding data centers at the agency level by centralizing oversight of its existing contractor-operated data center but did not provide supporting documentation. OPM reported that it has no new data centers. Therefore, we did not assess whether the requiring office and the relevant procurement official consult with the agency's Chief Information Officer (CIO) throughout the process of procuring a new data center or making substantial changes to an existing one. Also, we did not assess whether it uses commercial co-location services rather than building new data centers to the extent that it is cost-effective and meets agency mission needs.
Monitor data center operations	Partially addressed	For its existing data centers, OPM's performance work statement for its contractor-operated data center requires the use of automated tools to monitor the operations. Additionally, for its agency-operated data center the agency uses a spreadsheet to track the inventory of its physical data center's infrastructure. However, the spreadsheet does not demonstrate that OPM is using automated tools to monitor these data center operations. OPM reported that it has no new data centers. Therefore, we did not assess whether the agency incorporated automated tools into the management of all new data centers.
Incorporate energy and water usage into decision-making	—	OPM reported that it has no new data centers. Therefore, we did not assess whether the agency evaluated data centers against resource consumption metrics and best practices when making decisions. For its existing data centers, OPM officials stated that they incorporate efficiency requirements.
Meet mission availability requirements	Partially addressed	Officials stated that the agency has met mission availability and uptime requirements. OPM's *Performance Work Statement Data Center Hosting Services for Office of Personnel Management* includes service level requirements, including uptime requirements for its contractor-operated data center. However, this document did not sufficiently demonstrate that the agency used the results of a business impact analysis to set minimum availability requirements for each data center.
Meet information and physical security requirements	Partially addressed	OPM's performance work statement requires contractor-operated data centers to maintain information security protections and officials stated those requirements are being met. However, for both its new and its existing data centers, the agency did not provide documentation to demonstrate that the CIO works in coordination with other senior officials for security and facilities management within their agency to complete the Interagency Security Committee risk management process.

Fully addressed: The agency fully addressed all of the requirement's evaluation criteria; Partially addressed: The agency fully or partially addressed some, but not all of the requirement's evaluation criteria; Not addressed: The agency did not address any of the requirement's evaluation criteria; — = The requirement did not apply to the agency as it reported it had no new data centers and because the Office of Management and Budget did not specifically require agencies to apply the requirement to existing data centers.

Source: GAO analysis of Office of Personnel Management documentation. | GAO-27-108971

Small Business Administration

Table 24: Extent to Which Small Business Administration (SBA) Addressed the Five Office of Management and Budget Acquisition and Operational Data Center Requirements, as of August 2026

Requirement	Assessment	Summary of assessment
Make key data center decisions at the agency level	Partially addressed	SBA officials stated that all data center acquisition decision-making and operational management have been centralized in the Office of the Chief Information Officer (CIO) but did not provide supporting documentation. SBA reported that it has no new data centers. Therefore, we did not assess whether the requiring office and the relevant procurement official consult with the agency's CIO throughout the process of procuring a new data center or making substantial changes to an existing one. Also, we did not assess whether it uses commercial co-location services rather than building new data centers to the extent that it is cost-effective and meets agency mission needs.
Monitor data center operations	Not addressed	For its existing data centers, the agency did not state whether it adopted the use of automated tools to monitor the operation of its data centers to the extent that it was cost-effective. SBA officials stated that the agency plans to close all data centers by the end of October 2026. SBA reported that it has no new data centers. Therefore, we did not assess whether the agency incorporated automated tools into the management of all new data centers.
Incorporate energy and water usage into decision-making	—	SBA reported that it has no new data centers. Therefore, we did not assess whether the agency evaluated data centers against resource consumption metrics and best practices when making decisions.
Meet mission availability requirements	Partially addressed	SBA officials stated that in fiscal year 2025, the agency determined availability requirements and identified risks to availability of all agency-operated data center environments. SBA officials stated that in fiscal year 2026, it was executing migration of all remaining data center workloads to cloud environments, which would eliminate the agency-operated data center footprint entirely upon completion. However, the agency did not provide supporting documentation that demonstrated that the agency used the results of a business impact analysis to set minimum availability requirements.
Meet information and physical security requirements	Partially addressed	SBA officials stated that the agency adheres to the Interagency Security Committee risk management process and associated physical security standards for both internally managed and co-location data centers. However, for both new and existing data centers, the agency did not provide documentation to demonstrate that the CIO works in coordination with other senior officials for security and facilities management within their agency to complete the Interagency Security Committee risk management process.

Fully addressed: The agency fully addressed all of the requirement's evaluation criteria; Partially addressed: The agency fully or partially addressed some, but not all of the requirement's evaluation criteria; Not addressed: The agency did not address any of the requirement's evaluation criteria; — = The requirement did not apply to the agency as it reported it had no new data centers and because the Office of Management and Budget did not specifically require agencies to apply the requirement to existing data centers.

Source: GAO analysis of Small Business Administration documentation. | GAO-27-108971

Social Security Administration

Table 25: Extent to Which Social Security Administration (SSA) Addressed the Five Office of Management and Budget Acquisition and Operational Data Center Requirements, as of August 2026

Requirement	Assessment	Summary of assessment
Make key data center decisions at the agency level	Fully addressed	SSA's *Data Center Strategic Plan* and information technology procurement policy states that the Chief Information Officer (CIO) is responsible for making key data center decisions. SSA reported that it has no new data centers. Therefore, we did not assess whether the requiring office and the relevant procurement official consult with the agency's CIO throughout the process of procuring a new data center or making substantial changes to an existing one. Also, we did not assess whether it uses commercial co-location services rather than building new data centers to the extent that it is cost-effective and meets agency mission needs.
Monitor data center operations	Fully addressed	For its existing data centers, SSA's *Data Center Strategic Plan* states that the agency is using automated tools, such as the Data Center Infrastructure Management system to report on metrics for data centers. SSA officials stated that the agency monitors data center operations of agency-operated data centers, and it does not have any contractor-operated data centers. They also stated that SSA is establishing an automated method to report on servers. SSA reported that it has no new data centers. Therefore, we did not assess whether the agency incorporated automated tools into the management of all new data centers.
Incorporate energy and water usage into decision-making	—	SSA reported that it has no new data centers. Therefore, we did not assess whether the agency evaluated data centers against resource consumption metrics and best practices when making decisions. For existing data centers, SSA officials stated that the agency incorporates energy and water usage considerations into decision-making for its data centers.
Meet mission availability requirements	Fully addressed	SSA officials stated that the agency has met mission availability requirements including following modern software development practices to reduce impacts of data center downtime. Additionally, SSA's *Data Center Strategic Plan* states that a full-scale business impact analysis was conducted in 2009, 2012, and 2023. It also states that it includes resilience and risk aspects to its information technology Operations, Resilience, and Sustainability model. The agency demonstrated that it used the results of a business impact analysis to set minimum availability requirements for each data center. Specifically, the agency conducts business impact analyses to review its data centers and monitor mission-critical availability objectives and target thresholds.
Meet information and physical security requirements	Partially addressed	SSA officials stated that the agency follows Federal Information Security Modernization Act and Interagency Security Committee risk management processes to meet information and physical security requirements for its data centers. The agency conducts monthly data center meetings that include officials from the Office of the CIO and agency officials stated that it conducts facility security assessments every three years for each data center. However, it did not sufficiently demonstrate how the CIO is involved with senior officials for security and facilities management in completing the Interagency Security Committee risk management process.

Fully addressed: The agency fully addressed all of the requirement's evaluation criteria; Partially addressed: The agency fully or partially addressed some, but not all of the requirement's evaluation criteria; Not addressed: The agency did not address any of the requirement's evaluation criteria; — = The requirement did not apply to the agency as it reported it had no new data centers and because the Office of Management and Budget did not specifically require agencies to apply the requirement to existing data centers.

Source: GAO analysis of Social Security Administration documentation. | GAO-27-108971

Appendix III: Comments from the Social Security Administration

SOCIAL SECURITY
Office of the Commissioner

Carol C. Harris
Director, Information Technology and Cybersecurity Issues
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 "FEDERAL DATA CENTERS: Congress Has an Opportunity to Improve Agencies' Acquisition and Operations" (GAO-27-108971). We have no comments.

Please let me know if I can be of further assistance. Your staff may contact Amy Gao, Director of the Audit Liaison Staff.

Sincerely,

Chad Poist
Chief Risk Officer

SOCIAL SECURITY ADMINISTRATION BALTIMORE, MD 21235-0001

Appendix IV: GAO Contact and Staff Acknowledgments

GAO Contact

Carol Harris, harriscc@gao.gov

Staff Acknowledgments

In addition to the individual named above, the following staff made key contributions to this report: Niti Tandon (Assistant Director), Angela Watson (Analyst-in-Charge), Amanda Andrade, Sandra Kerr, Michael Lebowitz, Jacqueline Mai, Evan Nelson Senie, Walter Vance, and Adam Vodraska.

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, GAO posts on its website newly released reports, testimonies, and correspondence. You can also subscribe to GAO's email updates to receive notification of newly posted products.

Connect with GAO

Connect with GAO on X, LinkedIn, Instagram, and YouTube.
Subscribe to our 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

Media Relations

Sarah Kaczmarek, Managing Director, Media@gao.gov

Congressional Relations

David A. Powner, Acting Managing Director, CongRel@gao.gov

General Inquiries

https://www.gao.gov/about/contact-us



Please Print on Recycled Paper.