EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

January 14, 2025

M-25-03

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Clare Martorana
Federal Chief Information Officer

Clare A. Martorana

SUBJECT: Implementation Guidance for the Federal Data Center Enhancement Act

I. INTRODUCTION

Consistent with the Federal Data Center Enhancement Act of 2023 (FDCEA),[1] this memorandum provides guidance to Federal agencies on how to enhance the reliability and resiliency of agency data centers. It connects existing policies, risk management frameworks, and standards that agencies should use for the effective acquisition, design, and management of data centers and centralizes agency data center investment decisions.

Agency data centers must provide secure and highly available computing infrastructure to enable reliable access to Federal information and information systems. As agencies increasingly use digital services to make key processes more efficient, accessible, and scalable, maintaining reliable and secure data centers is even more critical. Additionally, advances in artificial intelligence (AI) capabilities and growing use of AI among agencies will further increase demand for high-performance computing provided by data centers.

As Congress acknowledged in enacting the FDCEA, the needs of the Federal Government with respect to data access and data processing systems have evolved since 2014, when the Federal Information Technology Acquisition Reform Act (FITARA) established the now-expired Federal Data Center Consolidation Initiative (FDCCI) in statute.[2] Given the significant efficiencies already achieved under that prior initiative, Congress did not renew the expired FDCCI provisions. Instead, it enacted the FDCEA, which struck the FDCCI provisions and directed OMB to set requirements for data centers to meet appropriate standards for cybersecurity, resiliency, and availability.[3] Prior OMB policy, such as memoranda implementing the FDCCI, provided a critical foundation for agencies to set data center

[1] National Defense Authorization Act for Fiscal Year 2024, Pub. L. No. 118–31 (2024 NDAA), §§ 5301-02 (2023).
[2] National Defense Authorization Act for Fiscal Year 2015, Pub. L. No. 113-291 (2015 NDAA), § 834.
[3] 2024 NDAA, §§ 5301-02 (amending 2015 NDAA, § 834 (44 U.S.C. § 3601 note)).

optimization metrics and move toward cloud and hybrid environments.[4] This memorandum builds on the best practice of optimizing an agency's data center footprint to meet its mission needs while implementing the new priority areas of the FDCEA.

II. SCOPE

A. Covered Agencies

This memorandum applies to all agencies listed in 31 U.S. Code § 901(b), part of the Chief Financial Officers (CFO) Act of 1990.

B. Covered Data Centers

This memorandum applies to agency data centers. For the purposes of this memorandum, a "data center" is:

1. Composed of one or more permanent or semi-permanent structures, or a dedicated space within such structure, that operates persistently in a fixed location;
2. Used for the housing of information technology (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.

This memorandum does not apply to structures or spaces that are exclusively used to host IT support infrastructure devices and capabilities, such as networking and telecommunications equipment, cabling, power and power distribution, print servers, or Internet of Things devices.

This memorandum applies only to agency-operated and contractor-operated data centers. A data center is "agency-operated" if it is owned, operated, or maintained directly by a covered agency. This includes facilities leased directly by an agency or those occupied under a General Services Administration (GSA) occupancy agreement. A data center is "contractor-operated" if it is owned, operated, or maintained by a contractor on behalf of a covered agency. Contractor-operated data centers can include commercial "co-location," in which an agency is one among many tenants.

Often it will not be practicable for an agency to apply the requirements of this memorandum to a private data center whose connection to the agency consists solely of supporting commercial cloud services or products that are provided to a wide variety of customers, including the agency. Accordingly, consistent with the FDCEA,[5] this memorandum does not apply to such a data center, unless the agency determines in a particular case both that the data center qualifies as "contractor-operated," as defined here, and that applying the memorandum's requirements to that data center is, in fact, practicable. If that presumption is

[4] *See:* OMB Implementation Guidance for the Federal Data Center Consolidation Initiative (FDCCI), March 2012; OMB Memorandum M-16-19, *Data Center Optimization Initiative (DCOI*) (rescinded in 2019); OMB Memorandum M-19-19, *Update to Data Center Optimization Initiative (DCOI)* (expired on September 30, 2022 via M-21-05)*;* OMB Memorandum M-21-05, *Extension of Data Center Optimization Initiative (DCOI).*

[5] 2024 NDAA, § 5302(b)(1) (amending 2015 NDAA, § 834(a)(3) to add the term "new data center" and define it to include contractor-operated data centers "to the extent practicable").

true, then the entity is not operating the center on the agency's behalf within the meaning of this memorandum, and this memorandum does not apply to the data center.

Some provisions of this memorandum apply differently depending on whether a given data center is new or existing. A data center is "new" for the purposes of this memorandum if it is established or substantially upgraded or expanded after the date of this memorandum. Substantial upgrades or expansions are 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 does not qualify as "new," it is considered an "existing" data center.

C. Effective Dates

Agencies must satisfy the applicable requirements of this memorandum with respect to new and existing agency-operated data centers within one year of the date of this memorandum. With respect to contractor-operated data centers, agencies must, to the greatest extent practicable, satisfy this memorandum's requirements by the later of the following two dates: (1) the date that is one year after the date of this memorandum; or (2) the date after the issuance of this memorandum that the contract for ownership, operation, or maintenance of the data center is first renewed, extended, or replaced.

III. REQUIREMENTS FOR ACQUIRING AND OPERATING FEDERAL DATA CENTERS

For existing data centers, agencies should take steps to assess gaps in their delivery of secure and reliable information systems that are caused by data centers not maintaining the appropriate capabilities. Agencies should appropriately account for these gaps in planning and budgeting for new data centers that can adequately meet the needs of agency information and information systems; however, given the potential significant cost of changing or acquiring new data centers, each covered agency is responsible for the prioritization of any transition.

A. Making 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 data centers, 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 towards the most efficient, reliable, and secure outcomes for the agency, while integrating data center and related IT portfolio decision-making and planning into the requisite acquisition, budget, and programmatic processes.

For both new and existing data centers, the requiring office and the cognizant 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. CIOs should be involved in all relevant budget and acquisition processes. 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.[6]

B. Monitoring 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 Information Management (DCIM) 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 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.

C. Incorporating 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 (CSO) and the agency's facilities management representatives.

D. Meeting 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. These risks to availability could vary greatly depending on the facility and its location, and therefore this policy does not provide an exhaustive list. Instead, agencies shall adopt a risk management-based approach to identify, reduce the likelihood of, and mitigate risks to the availability of data centers.[7]

[6] *See* NDAA 2015, as amended, § 834(b)(6)(B) (44 U.S.C. § 3601 note).

[7] Nothing in this policy should be construed to conflict with an agency's responsibilities to execute continuity of operations planning in accordance with OMB Directive D-16-1, *Minimum Requirements for Federal Executive Branch Continuity Communications Capabilities*.

1. Implement internal control policy to determine and meet data center availability requirements

Agencies are currently required to categorize Federal information and information systems based on the predicted impact of a loss of the information's or system's confidentiality, integrity, or availability.[8] Agencies must use a similar approach to help determine appropriate availability requirements for each agency- or contractor-operated data center that hosts Federal information or information systems.[9]

For both new and existing data centers, agencies must have an internal control process for managing risks to data center availability that includes the following activities:

- **Determine Availability (Uptime) Requirements**

  In order to effectively set data center availability requirements, agencies must first understand the availability needs of their information and information systems. A single availability requirement for all data centers would not align with the real-world environment in which they operate. Instead, agencies' disparate missions create varying needs for the availability of their information and information systems. To understand this need, agencies must use the results of 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. The Business Impact Analysis identifies the impacts of information system downtime on agency missions.[10] 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.

- **Identify Risks Affecting Availability**

  Data centers are complex environments with a number of external dependencies and internal equipment, any of which could cause downtime in multiple ways. Availability and uptime can be impacted by events such as environmental factors, natural disasters, power and equipment failures, and maintenance activities. Understanding the frequency and likelihood of these risks to availability is critical to managing them. Agencies must adopt the ongoing use of appropriate risk management frameworks to identify these risks and assess their likelihood.[11]

[8] *See* FIPS-199: Standards for Security Categorization of Federal Information and Information Systems.

[9] Uptime is typically expressed on an annual basis, and is equal to the total time in a year minus the sum of all planned and unplanned data center downtime. "Downtime" is any interruption of access to hosted information systems or information caused by data center equipment or operations. Availability is uptime divided by the total time in a year and multiplied by 100 to yield a percentage.

[10] *See* NIST SP 800-34 Rev 1 Contingency Planning Guide for Federal Information Systems

[11] *See* NIST SP 800-37 Rev. 2 Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy; NIST SP 800-30, Guide for Conducting Risk Assessments.

- **Implement Risk Avoidance and Mitigation Controls**

  Once agencies understand the nature, potential impact, and probability of risks to availability, it is important to either reduce the likelihood of those risks or mitigate the impact they may have. To the extent practicable, agencies must implement controls that will reduce or mitigate known risks to data center availability. Such controls should come from existing Federal publications or industry best practices.[12] Examples include multiple power transmission paths, continuous maintenance, and equipment redundancy or failover. Additionally, as appropriate, agencies should further control risk by geographically distributing their data centers to reduce the likelihood of a single event affecting multiple data centers.

2. Optimize Planned Downtime for Data Center Maintenance

Scheduled maintenance of data center equipment and related infrastructure can result in downtime for hosted information systems and the inaccessibility of stored information. Where feasible and cost-effective, agencies should implement data center maintenance practices that minimize planned downtime for hosted information systems. Such practices may include redundancy, load balancing, automated failover, and automation.

3. Follow Modern Software Development Practices to Reduce Impacts of Data Center Downtime

Data center availability is a contributing factor to overall information systems availability; however, infrastructure is not the only contributing factor. Developing software in a manner that accounts for possibly unreliable or ephemeral infrastructure provided by cloud hosting, commonly called "cloud-native" development, is a best practice for building resilient and reliable information systems. Agencies should prioritize modern software engineering practices that make information systems resilient against potential failures by associated infrastructure. Such practices are found to regularly reduce system downtime and associated costs. Following these principles may allow agencies to avoid the need for costly availability mitigations within the data center by engineering those mitigations into the information systems themselves. Agencies should regularly assess their application portfolio for opportunities to adopt modern software development practices both strategically and tactically.

E. Meeting Information Security 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 the appropriate information security and physical security protections. The Federal Information Security Modernization Act

[12] *See, e.g.*, National Institute of Standards and Technology (NIST), *Cybersecurity Framework 2.0*; NIST Special Publication (SP) 800-53, Rev. 5: *Security and Privacy Controls for Information Systems and Organizations* (2020); Telecommunications Industry Association, ANSI/TIA-942: *Telecommunications Infrastructure Standard for Data Centers*; Uptime Institute, *Data Center Site Infrastructure Tier Standard: Topology*.

(FISMA) assigns agency heads the ultimate authority and responsibility to develop and implement agency-wide information security programs.[13] Effective implementation of FISMA, including the appropriate use of NIST frameworks and security controls, should guide agencies in protecting the information and information systems stored within a data center.[14] 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.

Because data centers consist of independent building(s) with highly individualized infrastructure and equipment, they present unique physical security challenges. It is imperative that data center facilities have appropriate mitigations to protect against physical intrusions since such mitigations may go beyond the scope of the NIST SP 800-53 framework. For both new and existing data centers, agencies must follow the Interagency Security Committee (ISC) risk management process to determine the physical security needs for each data center facility and to implement the appropriate standards for countermeasures.[15] 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.

IV. REPORTING

In accordance with the FDCEA, agencies must report information on compliance with this memorandum's requirements to OMB, some of which will be made available to the public online. OMB will provide subsequent reporting instructions to agencies specifying the timing, format, and contents.

In addition, pursuant to the FDCEA, when an agency plans to make a management or financial decision during the development and planning lifecycle of a *new* data center that qualifies as a major acquisition, the agency must submit a written notification to the Office of the Federal Chief Information Officer, the Committee on Homeland Security and Governmental Affairs of the Senate, and the Committee on Oversight and Accountability of the House of Representatives.[16] The timing of notice is at the agency's discretion given the variety of "management or financial decisions" that may fall into this notification requirement. Agencies will be able to provide notice of these decisions to the OMB, barring any disclosure of sensitive information, as part of the data collection described previously.

V. SUNSET

In accordance with the FDCEA, the provisions in this memorandum, unless other specified, will expire on September 30, 2026.

[13] 44 U.S.C. § 3554.
[14] *See* NIST SP 800-53.
[15]*See* Executive Order 14111, *Interagency Security Committee*; U.S. Department of Homeland Security Cybersecurity & Infrastructure Security Agency & Interagency Security Committee, *The Risk Management Process: An Interagency Security Committee Standard* (2024).
[16] Pub. L. No. 118–31, the Federal Data Center Enhancement Act of 2023 (FDCEA). *See* OMB Circular No. A-11, part 7, section 300.4 for the definition of "major acquisition."