FDCEA Compliance Report

Agency	Reporting Period	Applicable Agency Data Centers	CIO Decision Centralization	CIO Decision Centralization Explanatory Statements	Availability (uptime) Internal Control Process Maturity	Availability (uptime) Internal Control Process Explanation	ISC (physical security) Adherence	ISC (physical security) Adherence Explanation
Department of Agriculture	July 2025	Yes	Yes		Yes, the implemented risk avoidance and mitigation controls to meet availability targets have been FULLY implemented.		Yes	
Department of Commerce	July 2025	Yes	Partially	The Commerce has selected 'Partially' because one of its bureaus' operational management processes is decentralized. It has drafted a policy regarding this requirement, and the policy memorandum is expected to be finalized in the coming weeks. However, the decision-making process for data center acquisitions is centralized. The CIOs make all decisions regarding the acquisition of data centers.	Yes, the implemented risk avoidance and mitigation controls to meet availability targets have been FULLY implemented.		Yes	
Department of Defense	July 2025	Yes	Yes		Yes, the internal control process under development to evaluate data centers has been PARTIALLY implemented.		Yes	
Department of Education	July 2025	No						
Department of Energy	July 2025	Yes	Partially	The agency has a well-established process to provide guidance and oversight across the enterprise. This ensures that the DOE Chief Information Officer (CIO) is adequately involved in planning, budgeting, and executing information technology acquisitions. This involvement aligns with the Federal Information Technology Acquisition Reform Act (FITARA) and OMB guidance on the management and oversight of information technology. We will follow up with sites that reported either partial or no CIO involvement for further clarification.	No, the process to evaluate data center availability is not implemented.	The majority of data centers have implemented an internal control process consistent with M-25-03 to manage data center availability risks. A limited number of sites indicated the absence of an availability/uptime control process for their data centers. We will seek clarification from those sites that reported non-adherence or partial adherence to M-25-03.	Yes	Nearly every data center adheres to the Interagency Security Committee (ISC) risk management process. We intend to follow-up with the outliers that reported 'no' or 'partially' for clarification.

Agency	Reporting Period	Applicable Agency Data Centers	CIO Decision Centralization	CIO Decision Centralization Explanatory Statements	Availability (uptime) Internal Control Process Maturity	Availability (uptime) Internal Control Process Explanation	ISC (physical security) Adherence	ISC (physical security) Adherence Explanation
Department of Health and Human Services	July 2025							
Department of Homeland Security	July 2025	Yes	Partially	DHS has a centralized acquisition called the Data Center and Cloud Optimization (DCCO) and a program office under the CIO to manage this acquisition. Data Center management of a 68,000 square foot data center is done through DCCO, and colocation sites can also be purchased through this centralized acquisition. However, some purchasing of Data Center colocation sites does not use DCCO. As part of FDCEA compliance, DHS plans to gain more centralized visibility into these colocation sites purchased outside of DCCO. Additionally, at the agency level, DHS Directive 142-02 establishes the responsibilities of the DHS CIO and DHS Component CIOs regarding IT integration and management. This includes the DHS-wide IT Acquisition Review (ITAR) process, which implements the oversight requirements of the Federal Information Technology Acquisition Reform Act. All program offices are required to submit an ITAR to the DHS OCIO for IT acquisitions more than $2.5M. This includes any data center acquisitions. However, there may be acquisitions below $2.5M for colocation sites.	Yes, executing internal control process to evaluate data center availability needs and risks affecting availability has been PARTIALLY implemented.	For DHS HQ's primary data center, Enterprise Data Center 1 or DC1, this is fully implemented. The data center owner (NASA) and DHS have established internal control processes to manage risks to availability as documented in CONOPS and various SOPs. The data center meets Uptime Institute Tier 3 N+1 requirements for availability, redundancy, diversity and failover with redundant power capability and network circuit carrier and path diversity, and access to multiple power grids as well as a robust generator back up capacity. NASA also closely monitors energy efficiencies, and DC1 has improved its power utilization efficiency (PUE) over the past decade or more. For DHS commercial colocations sites (e.g. Equinix), the data centers typically undergo independent assessments on a regular basis to ensure they also meet Tier 3 requirements with the infrastructure and processes in place to manage availability risks. However, some of these colocation sites may not fully meet the requirements described in the M-23-03 memo.	Partially	For DC1, this is fully implemented. DHS HQ has Common Controls which are assessed by DHS every 3 years and are included in the ATO (Authority to Operate). These include all aspects related to physical security of the data center and are in-line with Interagency Security Committee (ISC) processes. For DHS commercial colocation sites, typically independent assessments are performed regularly which cover areas of physical security. However, some colocations sites may not fully meet the requirements described in ISC risk management process.

Agency	Reporting Period	Applicable Agency Data Centers	CIO Decision Centralization	CIO Decision Centralization Explanatory Statements	Availability (uptime) Internal Control Process Maturity	Availability (uptime) Internal Control Process Explanation	ISC (physical security) Adherence	ISC (physical security) Adherence Explanation
Department of Housing and Urban Development	July 2025	Yes	Yes		Yes, the implemented risk avoidance and mitigation controls to meet availability targets have been FULLY implemented.		Yes	
Department of Justice	July 2025	Yes	Yes		Yes, executing internal control process to evaluate data center availability needs and risks affecting availability has been PARTIALLY implemented.	The Department developed an updated policy document on data centers consistent with M-25-03 that will be issued later this calendar year.	Yes	
Department of Labor	July 2025	Yes	Yes		Yes, executing internal control process to evaluate data center availability needs and risks affecting availability has been PARTIALLY implemented.	The controls and monitoring necessary for the uptime and availability of facility services for DOL's physical datacenter are FULLY in place. Work is ongoing to evaluate and implement mitigations for some core IT services that operate within the data center.	Yes	
Department of State	July 2025	Yes	Yes		Yes, the implemented risk avoidance and mitigation controls to meet availability targets have been FULLY implemented.		Yes	
Department of the Interior	July 2025	Yes	Partially	Acquisition is consolidated not operations. DOI-OCIO is beginning to consolidate hosting operations as part of the Executive Order 14210, Implementing the President's 'Department of Government Efficiency' Workforce Optimization Initiative and DOI's Secretarial Order 3429 to consolidate, unify and optimize DOI's costly hosting infrastructure.	Yes, executing internal control process to evaluate data center availability needs and risks affecting availability has been PARTIALLY implemented.	The internal control process is being finalized, and the operational implementation is partially implemented, but does not yet meet the criteria for fully implemented at this time.	Yes	
Department of Transportation	July 2025	Yes	Yes	The DOT CIO has appropriate decision-making authority consistent with existing law. The CIO collaborates with its Components on data center investments such that resulting decisions reflect the concurrence of the parties involved and exercise relevant legal authorities appropriately.	Yes, the internal control process under development to evaluate data centers has been PARTIALLY implemented.		Yes	

Agency	Reporting Period	Applicable Agency Data Centers	CIO Decision Centralization	CIO Decision Centralization Explanatory Statements	Availability (uptime) Internal Control Process Maturity	Availability (uptime) Internal Control Process Explanation	ISC (physical security) Adherence	ISC (physical security) Adherence Explanation
Department of Treasury	July 2025	Yes	Partially	Treasury has multiple centralized review process for looking at all IT acquisitions across the agency – data centers are just one element of those reviews.	Yes, the internal control process under development to evaluate data centers has been PARTIALLY implemented.	Each of Treasury's data centers is managed and operated in accordance with the operational, security and availability requirements mandated by the workloads the data center houses. The management of these data centers is federated however, to the Bureau that owns the data center. We do not currently have a centralized process for managing department-wide availability. This is within scope however, as Treasury develops and implements its shared services strategy.	Partially	Each of Treasury's data centers is managed and operated in accordance with the operational, security and availability requirements mandated by the workloads the data center houses. The management of these data centers is federated however, to the Bureau that owns the data center. We do not currently have a centralized process for managing adherence to ISC physical security requirements. That said, each of Treasury's data centers has been certified by its owner to meet the security, availability and operational requirements of its associated workloads and systems. For example, the IRS' data centers house Federal Taxpayer Information (FTI) which has its own legislated requirement on the housing and usage of that data. IRS' data centers have been certified to meet those more stringent requirements. As Treasury develops and implements its shared services strategy, FDCEA requirements for ensuring compliance with ISC requirements will be evaluated.
Department of Veterans Affairs	July 2025	Yes	Partially	VA does not have one centralized office that manages the 258+ data centers.	Yes, the implemented risk avoidance and mitigation controls to meet availability targets have been FULLY implemented.		Partially	Data centers have internal controls that only allow authorized personal access. ie PIV card readers that only allows authorized personnel. The Department remediates any deficiencies in accordance with agency policy.
Environmental Protection Agency	July 2025	Yes	Yes		Yes, the implemented risk avoidance and mitigation controls to meet availability targets have been FULLY implemented.		Yes	
General Services Administration	July 2025	No						

Agency	Reporting Period	Applicable Agency Data Centers	CIO Decision Centralization	CIO Decision Centralization Explanatory Statements	Availability (uptime) Internal Control Process Maturity	Availability (uptime) Internal Control Process Explanation	ISC (physical security) Adherence	ISC (physical security) Adherence Explanation
National Aeronautics and Space Administration	July 2025	Yes	Partially	This has been met for IT investments but not for all real property physical data center investment decisions. NASA is working to update processes and procedures to support this.	Yes, executing internal control process to evaluate data center availability needs and risks affecting availability has been PARTIALLY implemented.	1. NASA implements internal control policy to determine and meet data center availability requirements through System Security Plans (SSP) and Risk Based Decision (RBD) process. 2. NASA has implemented optimized planned downtime for data center maintenance that factors in mission freeze schedules. 3. NASA follows modern software development practices to reduce impacts of data center downtime. Legacy software will be retooled or decommissioned as part of Application Rationalization and in support of the NASA Data Center Optimization Strategy (DCOS). 4. All the current risk management processes and tools in use are not yet centralized. There is an effort in progress to improve this.	Partially	NASA meets the requirements for information security for most of the data center physical security requirements but not all. For example, some data centers are lacking physical controls due to funding shortfalls (e.g. security cameras).
National Science Foundation	July 2025	Yes	Yes		Yes, executing internal control process to evaluate data center availability needs and risks affecting availability has been PARTIALLY implemented.		Yes	
Nuclear Regulatory Commission	July 2025	Yes	Yes		Yes, executing internal control process to evaluate data center availability needs and risks affecting availability has been PARTIALLY implemented.	NRC is in the process of expanding its co-location footprint and relocation of mission critical assets into highly available data center co-locations to address availability needs.	Yes	
Office of Personnel Management	July 2025	No						
Small Business Administration	July 2025							
Social Security Administration	July 2025	Yes	Yes		Yes, the implemented risk avoidance and mitigation controls to meet availability targets have been FULLY implemented.		Yes	
U.S. Agency for International Development	July 2025							