3.   **Data Servers And Data Centers Approval Process**.

3.1.   **AF Data Center Infrastructure Management**. Under the FDCCI, OMB defines a data center as a closet, room, floor or building for the storage, management, and dissemination of data and information. This definition has been further defined by the DOD CIO to include single and multiple server instantiations regardless of adherence to Uptime Institute or TIA-942 standards. While it is generally recognized that weapon systems may not be data centers, most weapon systems have an IT component that may constitute a data center or reside in a data center. Thus, a weapon system designation , in and of itself, does not justify an exemption from FDCCI, related data center legislation, DOD guidance, or the guidance contained in this AFI. The SAF/CIO A6 will oversee management and disposition of all AF data centers under the purview of aforementioned guidance, to include the data center components of weapons systems.

3.2.   **AF Data Center Consolidation**. The DOD CIO, working under the purview of FDCCI guidance, requires all data centers (exceptions are noted below) to be documented in DCIMS. Records will be created and maintained by data center owners IAW guidance and training provided by the AF Data Center Consolidation team within SAF/CIO A6. Data center end states (discussed below) submitted by data center owners will be adjudicated and approved by SAF/CIO A6.

   3.2.1.   DCIMS Exemptions. The following items are exempt from FDCCI and do not require entry into DCIMS:

      3.2.1.1.   IT components constituting a data center that are onboard airborne platforms.

      3.2.1.2.   IT components constituting a tactical data center such as those contained in shelters.

      3.2.1.3.   IT components constituting a data center where the metadata (location, configuration, owner, etc.) is classified. Those systems are inventoried separately by the Director of National Intelligence.

   3.2.2.   Data Center End States. The following data center end states are defined by the DOD CIO and approved for use in DCIMS:

      3.2.2.1.   Core Data Center (CDC) – These locations are selected by the DOD CIO and operated by DISA.

      3.2.2.2.   Installation Processing Node (IPN) – Data centers required to host applications required for base operations where access does not transit the base boundary.

IPNs will not allow connections from one base to another and there shall be no more than one (1) IPN per base or installation.

3.2.2.3.   Special Purpose Processing Node (SPPN) – Servers connected to special purpose IT or non-IT equipment that cannot be moved due to technical requirements (such as flight simulators) or servers hosting applications critical to Air Force, DOD, or combatant command missions.

3.2.2.4.   Closed – Data centers not identified as one of the three categories above must be projected to close no later than 2018. Applications hosted within these data centers must be migrated to a data center approved by SAF/CIO A6 as noted below.

3.2.3.   Application Designations. Applications and/or systems that do not require base boundary transit for use are designated local and may reside in an IPN approved by SAF/CIO A6. All other applications and/or systems are designated enterprise and must be hosted in an enterprise data center approved by SAF/CIO A6 NLT 4th quarter of Fiscal Year 2018 (QTR4FY18). Exceptions may be granted by SAF/CIO A6 for those instances where migration to an enterprise location would introduce risk to mission or an approved business case analysis shows migration to be cost prohibited. Application owners must coordinate with appropriate organizations as directed in Air Force Guidance Memorandum 33-04, Common Computing Environment.

3.2.3.1.   DISA Core Data Center/MilCloud (any app, system, or service).

3.2.3.2.   Commercial Cloud (any app, system, or service) with a DoD Provisional Authorization for the corresponding data level.

3.2.3.3.   IPNs approved by SAF/CIO A6 (base local apps only).

3.2.3.4.   SPPNs approved by SAF/CIO A6 (SPPN specific apps only).

3.3.   **Obligation of Funds Related to Data Centers (10 USC §2223a, Data Servers and Centers)**. Obligations, regardless of appropriation, other required approvals, or other granted authorities to acquire servers and/or equipment related to data centers (items specified below) as defined above must be approved by SAF/CIO A6 prior to execution. Exemptions are outlined below; however, data centers exempted under 10 USC §2223a, Data Servers and Centers must still be documented within the DCIMS, including IT components of weapons systems.

3.3.1.   Exemptions to 10 USC §2223a, Data Servers and Centers:

3.3.1.1.   Items acquired using National Intelligence Program (NIP) funds. This does not include Military Intelligence Program fund.

3.3.1.2.   Items acquired using High Performance Computing Modernization Program (HPCMP) funds.

3.3.1.3.   Items within data centers exempted from FDDCI as described in paragraph 3.2.1.

3.3.2.   Items Covered Under 10 USC §2223a, Data Servers and Centers. This guidance applies to obligations of any and all funds to: construct or modify existing data center buildings, facilities, or rooms; or acquire items in the categories listed below regardless of appropriation, requirement, and/or originator.

    3.3.2.1.   Servers of any type.

    3.3.2.2.   Server software of any type.

    3.3.2.3.   Virtual Suites.

    3.3.2.4.   Storage to include Storage Area Networks (SAN), Network Attached Storage (NAS), and Direct Attached Storage (DAS).

    3.3.2.5.   Racks.

    3.3.2.6.   Uninterruptable Power Supply (UPS).

    3.3.2.7.   Generators.

    3.3.2.8.   Routers, switches, etc. (unless deployed in a facility separate from a data center or servers such as a wiring closet).

    3.3.2.9.   Cooling systems and environmental monitoring capabilities.

    3.3.2.10.   Backup capabilities, regardless of medium.

    3.3.2.11.   End user devices (e.g., desktops, laptops, tablets, mobile devices), and associated software and services used within a data center.

    3.3.2.12.   Service, support, and maintenance contracts (e.g., warranty support, preventive, routine, and emergency maintenance) for existing data center capabilities.

3.4.   **Data Servers and Centers Submission Preparation**. Requests for obligation authority under 10 USC §2223a, Data Servers and Centers, must support a data center having an approved record in the DCIMS with a valid DOD identification number. All data centers must also have a corresponding and populated record in the Enterprise Information Technology Data Repository (EITDR). All requests for obligation authority and queries, to include requests for templates or support, must be submitted to the SAF/CIO A6 DCC team via the MAJCOM or FOA A6 to the AF Data Center Consolidation organizational mailbox: usaf.pentagon.saf-cio-a6.mbx.a3c-a6c-afdcc-workflow@mail.mil.

3.5.   **Data Servers and Centers Submission Process**. Organizations must submit a spend plan for each data center maintained in DCIMS NLT 31 July of each year. Data centers in DCIMS without an approved spend plan on file with SAF/CIO A6 will be considered noncompliant. Spend plans must detail individual acquisitions for items listed in paragraph 3.3.2 planned for the upcoming year and provide the information listed below in paragraphs 3.5.1-3.5.7. Organizations requiring acquisition of items not detailed on approved spend plans must submit an out of cycle request for approval to include the items listed below in paragraphs 3.5.1-

3.5.7. Spend plans will be approved annually by SAF/CIO A6 to satisfy requirements under the purview of 10 USC §2223a:

3.5.1.   Obligation Detail Matrix (format provided by SAF/CIO A6 DCC team).

3.5.2.   Brief description for each acquisition.

3.5.3.   A description of how each acquisition supports consolidation of infrastructure (FDCCI) and the JIE.

3.5.4.   Individual purchase request or spreadsheet that shows item, quantity, and unit cost for each acquisition.

3.5.5.   An approval memo signed by the wing commander, MAJCOM A6, PMO, or PEO and the approver/signer must be O6/GS-15 or higher. Approval memos must also certify that no capability exists within the base, MAJCOM, or program to satisfy the approved requirement.

3.5.6.   All spend plans against a data center with an end state of "Closed" must be accompanied by an approved POAM, which clearly depicts closure before end of FY18. Moreover, the acquisitions for these data centers must clearly depict actions to realize closure.

3.5.7.   A description of efficiencies realized including current and project savings in dollars or personnel, reduction in required floors space, or reduction in energy usage.

3.6.   **Approval Process and Timeline**. The SAF/CIO A6 goal for completing review and granting approval or disapproval is 10 working days; however, this can be affected due to unforeseen circumstances. The "10 day clock" starts when all required inputs have been received and validated from the requestor. An approval code assigned by SAF/CIOA6 is required prior to execution of contracts or obligation of any and all funds for each item relating to those described in paragraph 3.3.2. Approval codes and associated items will be listed on the Obligation Detail Matrix attached to the SAF/CIO A6 approved spend plan and sent to the requestor.

3.6.1.   Out of cycle approval codes may be obtained by sending an electronic message to the AF DCC Team at usaf.pentagon.saf-cio-a6.mbx.a3c-a6c-afdcc- workflow@mail.mil. Requests received prior to 1600 EST will generally be approved the same day with approval codes returned to the requestor. Requestors must present the validation e-mail provided by SAF/CIO A6 personnel via the "USAF Pentagon SAF-CIO A6 Mailbox A3C-A6C AFDCC Workflow" electronic mailbox along with the out of cycle approval code for funds to be obligated by a contracting officer. A SAF/CIO A6 approval memorandum and attached Obligation Detail Matrix must be provided for all obligations relating to items in paragraph 3.3.2, regardless of approval code disposition.

3.7.   **Requestor Reporting Requirements**. All changes to data center configurations (e.g. shutting down a data center) must be reported within 30 days of the event occurring. Actual obligation amounts must be reported within 30 days of the event occurring for each item on the Obligation Detail Matrix attached to approved spend plans. Failure to comply with these instructions or instructions issued in approval memoranda results in noncompliance for the data center.