CHIEF INFORMATION OFFICER

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

MEMORANDUM FOR SENIOR PENTAGON LEADERSHIP
COMMANDERS OF THE COMBATANT COMMANDS
DEFENSE AGENCY AND DOD FIELD ACTIVITY DIRECTORS

SUBJECT: Department of Defense Joint Warfighting Cloud Capability and Next Steps to Rationalize Cloud Use Across the Department of Defense

References: (a) DoD CIO Memorandum, "Updated Guidance on the Acquisition and Use of Commercial Cloud Computing Services," December 15, 2014
(b) DoD CIO Memorandum, "Interim Guidance for Implementation of the Department of Defense Cloud Strategy," April 16, 2020
(c) Section 1553 of the Fiscal Year 2023 National Defense Authorization Act

In December 2022, the Department of Defense (DoD) awarded the Joint Warfighting Cloud Capability (JWCC), which is a multi-vendor contract vehicle designed to meet DoD enterprise cloud requirements. The JWCC contract vehicle provides the DoD an unprecedented ability to directly acquire commercial capabilities and services at three classification levels (Unclassified, Secret, Top Secret), and from strategic and operational headquarters to the tactical edge. Further, the JWCC contract vehicle enables Department-wide adoption of commercial cloud services, procurement, provisioning, and cloud resources tracking through a single point of entry to ensure competition and enhance the Department's understanding of cloud requirements and assets throughout the DoD enterprise. The establishment of this long-awaited enterprise cloud contract capability provides the Department of Defense Chief Information Officer (DoD CIO), working in concert with DoD Component cloud managers and information technology leaders, the opportunity to begin rationalizing cloud activities within the DoD Component and across the Department in accordance with the guidelines set in this memorandum. The JWCC is not a cloud management or hosting environment, but rather a key vehicle in the Department's technology arsenal for the acquisition of services for current and future DoD Component managed and controlled cloud environments. This guidance rescinds references (a) and (b), apart from Attachment 2 of reference (b) which remains valid and is attached.

As a first step in this process, Office of the Secretary of Defense (OSD) Components, and Defense Agencies and Field Activities (DAFAs)[1] will use the JWCC contract vehicle for all available offerings to procure future enterprise cloud computing capabilities and services. All cloud capabilities and services currently under contract in OSD Components and DAFAs will transition to the JWCC vehicle upon expiration of their current period of performance. OSD Components and DAFAs may utilize on-premises cloud offerings (e.g., Stratus), where applicable.

[1] National Reconnaissance Office, National Geospatial-Intelligence Agency, Defense Intelligence Agency, and National Security Agency will continue to use the Intelligence Community's Commercial Cloud Enterprise (C2E) contract for their Intelligence mission's needs.

Additionally, all DoD Components, to include Military Departments (MILDEPs) and Combatant Commands (CCMDs), will leverage the JWCC contract vehicle for all available offerings for any new cloud computing capabilities and services at the Secret (Impact Level 6) or Top Secret, including all tactical edge and Outside the Continental United States (OCONUS) cloud computing capabilities and services.

MILDEPs and CCMDs may continue to procure cloud capabilities and services not covered above, to include Infrastructure as a Service (IaaS), through MILDEP cloud contract vehicles or vehicles other than JWCC. While not mandating JWCC use for all cloud capabilities and services, DoD CIO will encourage MILDEPs and CCMDs to consider use of JWCC for their needs, especially as trends from OSD Component and DAFA-use provide additional data points in the coming year on price competitiveness and mission efficacy.

Looking ahead, DoD CIO will restructure the DMI EXCOM governance by refocusing and renaming the forum to the DoD Information Enterprise Portfolio Management, Modernization and Capabilities Council (DoD-IE-PM2C). This is to provide a broader forum to continue with existing and expanding digital modernization activities relevant to the Department's information enterprise[2], including the current and future cloud initiatives as well as contractual efforts, and review of procurement administrative lead time for cloud initiatives. In addition, further guidance for incorporation of requirements into contracts for test and evaluation of classified clouds will be provided upon development of a policy and plan in accordance with reference (c). Immediately addressing governance is necessary in order to keep pace with the evolving information environment and the rapidly changing technology landscape in an ever-increasing digital battlefield.

The DoD-IE-PM2C will update the DMI EXCOM charter, and it will comprise representation from DoD Components and other agencies across the DoD to ensure effective cloud rationalization that balances each DoD Component's role for delivery of mission and warfighting effects. In order to rationalize cloud services and capabilities procurement and provisioning, all DoD Components will provide to DoD CIO the following information regarding current enterprise cloud contracts no later than 60 days from the issuance of this guidance and request:

a) Current Cloud Service Provider(s).
b) Acquisition vehicles presently being used for cloud capabilities and services.
c) Details regarding the cloud capabilities and services presently being procured, to include pricing.
d) Plans for obtaining future cloud capabilities and services, and whether likely through JWCC or another procurement vehicle.
e) Any current integrator or third-party reseller for cloud services and capabilities, and from whom the integrator or reseller is obtaining cloud capabilities and services.

DoD CIO, in coordination the DoD Components, will review and assess the above information in planning to continue to modernize and improve the Department's enterprise cloud

[2] DoD Directive (DoDD) 8000.01, Management of the Department of Defense Information Enterprise (DoD IE).

capabilities. This will inform the DoD's broader cloud ecosystem, mission requirements, and pricing, among other aspects.

The DoD CIO point of contact for this matter is [redacted]

John B. Sherman

Attachment:
As stated

Attachment

DOD CLOUD CONTRACT COMPLIANCE REQUIREMENTS

This attachment describes DoD cloud compliance requirements. It will be updated at https://www.cloud.mil as compliance requirements mature.

- **Defense Federal Acquisition Regulation Supplement (DFARS) Cloud Clause:** Contracts for cloud services will include the cloud policy and contract clauses defined in DFARS Subpart 239.76.

- **DoD Cloud Computing Security Requirements Guide (CC SRG):** DoD Components will comply with the requirements specified in the CC SRG and only use cloud services that have been granted a DoD provisional authorization at the appropriate Impact Level.

- **Penetration Testing:** Unclassified cloud services are required to undergo annual penetration testing in accordance with the FedRAMP process and the DoD CC SRG. In addition to the standard penetration testing, contract0s for classified cloud services must include provisions that enable DoD red teams to conduct independent, adversarial assessments of the cloud environment that emulate the most capable, nation-state threats.

- **System Network Approval Process (SNAP):** Cloud use will be registered in SNAP in accordance with the Defense Information Systems Network (DISN) Connection Process Guide and Joint Force Headquarters-DoD Information Network direction.

- **DoD Budget Reporting Guidance:** DoD Components will report cloud investments in the DoD Select & Native Programming Data Input System – Information Technology in accordance with DoD Budget Reporting Guidance.

- **Cloud Access Point (CAP):** Commercial cloud services used for Impact Level 4 or above must be connected to customers through the DISN Enterprise CAP or through a Component CAP solution approved by the DoD CIO.

- **DoD Instruction 8530.01, "Cybersecurity Activities Support to DoD Information Network Operations," July 25, 2017:** Cloud use will be supported by Cybersecurity Service Providers in accordance with DoD Instruction 8530.01.