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

CHIEF INFORMATION OFFICER

APR 16 2020

MEMORANDUM FOR CHIEF MANAGEMENT OFFICER OF THE DEPARTMENT OF DEFENSE
SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
CHIEF OF THE NATIONAL GUARD BUREAU
COMMANDANT OF THE UNITED STATES COAST GUARD
COMMANDERS OF THE COMBATANT COMMANDS
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
DIRECTOR OF COST ASSESSMENT AND PROGRAM EVALUATION
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
DIRECTOR OF OPERATIONAL TEST AND EVALUATION
ASSISTANT SECRETARY OF DEFENSE FOR LEGISLATIVE AFFAIRS
ASSISTANT TO THE SECRETARY OF DEFENSE FOR PUBLIC AFFAIRS
DIRECTOR OF NET ASSESSMENT
DIRECTORS OF DEFENSE AGENCIES
DIRECTORS OF DOD FIELD ACTIVITIES

SUBJECT: Interim Guidance for Implementation of the Department of Defense Cloud Strategy

The use of cloud capabilities is changing the way the DoD develops, deploys, and operates systems and services. The Department is building and scaling more effective cybersecurity, advanced analytical capabilities, better command and control, and future enabling technologies. As cloud adoption matures, the Department will improve the speed of software delivery, the organization of massive amounts of data, and will enable rapid access to information for improved decision making to preserve and extend our military advantage.

The DoD Cloud Strategy provides the Department unifying guidance to focus cloud computing investments on reducing inefficiencies and accelerating the Department's digital modernization efforts. The Department remains on a path toward a unified DoD Enterprise Cloud Environment (DECE), a multi-cloud, multi-vendor ecosystem of cloud services. With the delay in awarding the Joint Enterprise Defense Infrastructure (JEDI) Cloud and the Defense Enterprise Office Solution (DEOS) contracts, this memorandum provides interim guidance to ensure continued cloud adoption in alignment with the DoD Cloud Strategy.

DoD Components will prepare for adoption of the DECE by conducting system and application rationalization to identify systems and applications that are best postured to adopt cloud services. DoD Components are authorized and encouraged to use the cloud contracts and broker services identified in the attached list of approved cloud services to satisfy cloud computing requirements. Existing cloud contracts that comply with the requirements in the

attached cloud compliance requirements are approved to continue within existing contract scopes and periods of performance; however, consistent with the DoD Cloud Strategy, DoD Components should begin to reduce the number of cloud contracts through consolidation under broader enterprise contracts. DoD Components seeking to pursue new contracts will consult with the DoD Chief Information Officer (CIO) at DoDCIO.Cloud.Team@mail.mil and include a brief summary of contract scope and ceiling.

The Defense Agencies and Field Activities participating in the DoD CIO's Information Technology Reform initiatives will continue ongoing cloud adoption activities in accordance with DoD CIO Memorandum, "Fourth Estate Migration Plans," November 20, 2018.

Evolving guidance and related resources will be published at https://www.cloud.mil. The DoD CIO point of contact is Robert W. Vietmeyer, (571) 372-4461 or DoDCIO.Cloud.Team@mail.mil.

Dana Deasy

Attachments:
As stated

Attachment 1

DoD ENTERPRISE CLOUD ENVIRONMENT

In accordance with DoD Chief Information Officer (CIO) Memorandum, "Interim Guidance for Implementation of the Department of Defense Cloud Strategy," the Department will use the multi-cloud, multi-vendor offerings. These multi-cloud, multi-vender offerings are a group of contracted cloud services approved for use by mission owners or applicable communities to achieve the goals of the DoD Digital Modernization Strategy and do not require additional review or approval by the DoD CIO.

This attachment describes the current approved cloud services and will be updated at https://www.cloud.mil as related guidance evolve.

Enterprise contracts, such as milCloud 2.0, are available for use by all DoD Components. DoD Components may also use component and special-use cloud contracts that have been evaluated by the Office of the DoD CIO in meeting or exceeding the goals and objectives of the DoD Digital Modernization Strategy.

Enterprise Contracts:

Program Name	Service Type and Description	Entrance Point
milCloud 2.0	On-premises general purpose services managed by DISA.	https://www.milcloud2.mil/bp/

Component and Special-Use Cloud Contracts:

Program Name	Service Type and Description	Entrance Point
Air Force Cloud One	**AF provided cloud hosting service and platform, offering access to AWS and Azure environments.**	https://intelshare.intelink.gov/sites/AFCCE/Pages/Home.aspx https://software.af.mil/team/cloud-one/
Intelligence Community (IC) Cloud Services*	Cloud services provided by the Intelligence Community (IC) for use by the IC and those supporting an IC mission.	SIPR URL: http://www.sc2shome.sgov.gov/ JWICS URL: https://c2s.cia.ic.gov/

* In accordance with Defense Procurement and Acquisition Policy Memorandum, "Guidance on the Use of Intelligence Community Information Technology Enterprise Sponsored Contracts for DoD Activity Procurement Actions," February 27, 2015, DoD members of the Intelligence Community may consider IC Cloud Services as part of their business case analysis.

Attachment 2

DOD CLOUD CONTRACT COMPLIANCE REQUIREMENTS

In accordance with DoD Chief Information Officer (CIO) Memorandum, "Interim Guidance for Implementation of the Department of Defense Cloud Strategy," the Department will use a multi-cloud, multi-vendor approach to achieve the goals of the DoD Digital Modernization Strategy.

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 239.7600.

- **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, contracts 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 System 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.