



DEPARTMENT OF DEFENSE

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

CHIEF INFORMATION OFFICER

DEC 15 2014

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DEPUTY CHIEF MANAGEMENT OFFICER
COMMANDERS OF THE COMBATANT COMMANDS
DIRECTOR, COST ASSESSMENT AND PROGRAM EVALUATION
DIRECTOR, OPERATIONAL TEST AND EVALUATION
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
ASSISTANT SECRETARIES OF DEFENSE
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTOR, NET ASSESSMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: Updated Guidance on the Acquisition and Use of Commercial Cloud Computing Services

- References:
- (a) DoD Memorandum, "Designation of the Defense Information Systems Agency as the Department of Defense Enterprise Cloud Service Broker," June 26, 2012 (Canceled)
 - (b) DoD Memorandum, "Supplemental Guidance for the Department of Defense's Acquisition and Secure Use of Commercial Cloud Services," December 16, 2013 (Canceled)
 - (c) DoD Memorandum, "Use of Enterprise Information Technology Standard Business Case Analysis," October 23, 2014
 - (d) Federal Risk Authorization and Management Program, <http://cloud.cio.gov/fedramp>
 - (e) DoD Instruction 8500.01 "Cybersecurity", March 14, 2014

This memo clarifies and updates DoD guidance when acquiring commercial cloud services, and hereby cancels and replaces references (a) and (b). In the context of this memo, commercial cloud services also refer to cloud services provided by Non-DoD federal government organizations.

1. DoD components may acquire cloud services directly. It is no longer a requirement to use DISA for the acquisition of cloud computing services.
2. Each Component remains responsible for determining what data and missions are hosted by external cloud service providers per the direction below.
3. Each use of cloud services must be analyzed using the Enterprise IT Business Case Analysis (BCA) template as provided in reference (c). The BCA must be approved by

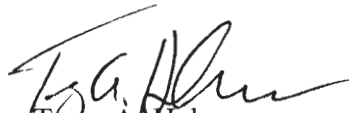
the Component CIO and a copy submitted to the DoD CIO. DISA provided cloud services must be considered as part of the BCA.

4. The Federal Risk Authorization and Management Program (FedRAMP) will serve as the minimum security baseline for all DoD cloud services as described in reference (d). Per current policy, components may host Unclassified DoD information that has been publicly released on FedRAMP approved cloud services.
5. For more sensitive DoD unclassified data or missions (called *Sensitive Data* below), DoD has developed cloud security requirements and guidance that go beyond FedRAMP. A draft of this *DoD Cloud Computing Security Requirements Guide* (the Guide) is currently out for DoD public comment, with official release scheduled for January 7, 2015. The Guide is intended to give cloud providers a stable security requirement, and to help DoD cloud customers move more rapidly and securely into the cloud. The Guide defines several classes of Sensitive Data, with increasing security requirements for each. Additional detail on the Guide and the Guide development process can be found in paragraph 11.
6. Any cloud service provider that is interested in hosting Sensitive Data will submit evidence to DISA that the provider meets specific requirements of the Guide. DISA will evaluate this evidence and if the provider meets the requirements, DISA will issue a DoD Provisional Authorization (PA). The PA will describe the types of information and mission that can be hosted by a particular cloud service.
7. Per the BCA of paragraph three, using the customer guidance in the Guide and the information in the PA, the CIO of each Component will determine which cloud service provider to use for a particular set of information or mission. DoD Components may only host Sensitive Data in cloud service providers that have an appropriate PA.
8. Commercial cloud services used for Sensitive Data must be connected to customers through a Cloud Access Point (CAP) provided by DISA or through a CAP provided by another DoD Component. All CAPs must be approved by DoD CIO. The current Navy CAP is an example of an approved provisional cloud access point. In the future, in order to standardize cyber defenses, our goal is that all DoD access to commercial cloud services be via a DISA provided CAP. This CAP will protect all DoD missions from incidents that affect a particular cloud service provider, and will provide perimeter defenses and sensing for applications hosted in the commercial cloud service.
9. Operations in a cloud environment are diverse and will require different concepts of operations (CONOPS), business strategies, etc. Components are responsible for cyberspace defense of all information and missions hosted in commercial cloud services, and will share cyberspace defense information as necessary and appropriate with cloud service providers, in accordance with reference (e). DoD Components that acquire or use cloud services are still responsible for ensuring that end to end security requirements are met. To operate and defend successfully, this will require collaboration and information sharing among the Component, DISA and the cloud service provider.

10. The *DoD Cloud Computing Security Requirements Guide* will be an evolving document informed by public and private input. It is intended to be a collaborative document between the government and private sector that recognizes the rapid technology and business changes in the cloud services environment. To assist in the development and use of the *DoD Cloud Computing Security Requirements Guide*, DoD will be holding a series of meetings, the first being a technical interchange meeting in person and via the web with interested DoD and industry partners on December 18, 2014. Comments on the draft *DoD Cloud Computing Security Requirements Guide* are due by December 29, 2014. Details can be found at http://iase.disa.mil/cloud_security/Pages/index.aspx. In January 2015, the Deputy CIO for Cybersecurity will host the first regular meeting with DoD and industry, at which time the organizations with key cloud responsibilities in DoD will describe DoD requirements, processes, and plans, and seek feedback from our government, private and public partners in the cloud environment. In addition, comments on the Guide are welcome at any time, via the following email address: disa.letterkenny.FSO.mbx.stig-customer-support-mailbox@mail.mil.

11. Additional information on procuring cloud services is provided in attachment (1).

DoD CIO point of contact for cloud is Robert Vietmeyer, robert.w.vietmeyer.civ@mail.mil, (571) 372-4461. The DISA point of contact is the Risk Management Office, disa.meade.ma.mbx.maops@mail.mil, (301) 225-7900.


Terry A. Halvorsen
Acting

Attachment:
As stated

ATTACHMENT 1

CLOUD SERVICE PROCUREMENT INFORMATION

DoD Components are responsible for acquiring the Information Technology (IT) services that meet their mission objectives and provide an optimal solution compliant with DoD cybersecurity requirements. Components will:

1. Address the contractual risks and issues associated with cloud services identified in the DoD Cloud Computing Issues matrix in all contracting vehicles that are used to acquire commercial cloud services, found at https://dodcioext.osd.mil/SitePages/Cloud_Computing.aspx. Defense Procurement and Acquisition Policy will develop appropriate contract language to address the issues, guidance and requirements in DFARS Case 2013-D024, Contracting for Cloud Services.
2. Register use of the Cloud Service Provider (CSP) in the DoD Information Technology Portfolio Registry (DITPR) and report its use as part of the Components Federal Information Security Management Act (FISMA) report.
3. Report all appropriate information within the Select and Native Programming Data Input System – Information Technology (SNaP-IT) as directed in DoD CIO annual IT budget guidance for each utilized cloud computing service.
4. Request exceptions to these requirements for commercial cloud services using the DoD Information Networks (DODIN) Waiver Process.
5. Track the evolution and use the latest versions of the references and any published concepts of operation in all new cloud deployments. Cloud services, DoD programmatic approaches to cloud services, technical approaches for connecting to cloud services, and operational approaches for defending DoD information and missions hosted in cloud services are all evolving continuously. To ensure dependable mission execution and information security, Components will use the most recent guidance, requirements and policies to support their cloud deployments.