



DEPARTMENT OF THE NAVY
CHIEF INFORMATION OFFICER
1000 NAVY PENTAGON
WASHINGTON DC 20350-1000

04 June 2013

MEMORANDUM FOR DISTRIBUTION

Subj: UPDATE TO DEPARTMENT OF THE NAVY APPROACH TO CLOUD COMPUTING

- Ref:
- (a) Department of Navy Chief Information Officer (DON CIO) Memorandum of April 1, 2012, Subj: Department of the Navy Approach to Cloud Computing
 - (b) Under Secretary of the Navy Memorandum of December 3, 2010, Subj: Department of the Navy (DON) Information Technology (IT)/Cyberspace Efficiency Initiatives and Realignment
 - (c) National Defense Authorization Act (NDAA) for Fiscal Year 2012, Section 2867
 - (d) DoD CIO, July 2012, Cloud Computing Strategy
 - (e) DoD CIO Memorandum of June 26, 2012, Subj: Designation of the Defense Information Systems Agency as the Department of Defense Enterprise Cloud Service Broker
 - (f) National Institute of Standards and Technology (NIST) 800-53, February 2012: Security and Privacy Controls for Federal Information Systems and Organizations
 - (g) Committee on National Security Systems Instruction (CNSSI) 1253, 15 March 2012: Security Categorization and Control Selection for National Security Systems
 - (h) DoD Enterprise Cloud Service Broker Cloud Security Model Version 1.0, 9 April 2013

This memorandum cancels reference (a) and provides updated Department of the Navy (DON) policy. Reference (b) directed the Department of the Navy Chief Information Officer (DON CIO) to lead the Department's Information Technology (IT) Efficiency Initiatives. To increase efficiency without sacrificing operational effectiveness; organizations, system/application owners and program managers must expand their analyses of alternatives for hosting DON systems and information to include Department of Defense (DoD) and commercial cloud service providers (CSPs). This approach is consistent with reference (c), which requires a Department of Defense-wide strategy to address the "Migration of Defense data and government-provided services from Department-owned and operated data centers to cloud computing services generally available within the private sector that provide a better capability at a lower cost with the same or greater degree of security." This approach is also in keeping with the DON's practice of hosting Navy Marine Corps Intranet (NMCI) data in commercial service provider facilities.

References (d) and (e) establish the Defense Information Systems Agency (DISA) as the Enterprise Cloud Service Broker. The Broker has reached Initial Operational Capability (IOC) and has the framework in place to support unclassified publicly releasable data. DISA, as the Project Management Office (PMO) for the Broker, used this framework to assess the first Federal Risk and Authorization Management Program (FedRAMP) authorized commercial

Subj: UPDATE TO DEPARTMENT OF THE NAVY APPROACH TO CLOUD COMPUTING

cloud offerings for DoD use. Until the Defense Information Assurance Certification and Accreditation Program (DIACAP) is replaced by the Risk Management Framework (which aligns with FedRAMP), Offices of the Designated Approving Authority (ODAA) will evaluate cloud services utilizing the current DIACAP. The Broker will evaluate CSPs against FedRAMP requirements and additional DoD overlay control requirements to identify compliance with applicable controls and support DON's assessment of residual risk. The evaluation criteria are available at http://iase.disa.mil/cloud_security/index.html . DON will work with DISA to continually improve the utility of FEDRAMP or DoD Controls to properly balance mission criticality, threats and operational risk through engagement with the appropriate governance structures.

The DON will leverage cost effective Broker-provided offerings and partner with DISA to accelerate availability of secure and less expensive commercial cloud information technology solutions and address the challenges associated with support for controlled unclassified information (CUI). The DON and DISA "early adoption" of commercial cloud services will pioneer the establishment of security, performance, and best value norms for this new category of IT service. DON CIO will work with the Broker PMO to establish a Military Department-level governance process to adjudicate requested exceptions to this policy.

As a first step, DON low-impact information systems and mission functions will move to commercial CSPs that meet mission and security requirements, unless a more cost effective DoD solution is identified. This enables compliance with reference (c) while achieving necessary cost savings. A low-impact system is defined in references (f) and (g) as an information system in which the loss of confidentiality, integrity, and availability could be expected to have limited adverse effect. DON organizations are to categorize as low-impact those publicly accessible information systems, applications, and websites that contain only information previously approved for public release.

The DON CIO will utilize the Broker to arrange for cost-effective offerings, via the Enterprise Cloud Service Catalog or other contract vehicles approved by the Broker, and will share information assurance assessments and Authority to Operate packages. Reciprocity of accreditation decisions and the artifacts supporting those decisions will be used to significantly reduce the time and expense of the DoD and Federal certification processes. Prior to any new cloud implementation, requesting organizations will contact the Broker in order to leverage accreditation artifacts from previous packages and to identify the need for additional security controls or verification testing. Contract, Performance Work Statement, and Service Level Agreement language related to cloud service terms of service and Information Technology Service Management attributes will be coordinated with the Broker and Acquisition Authority

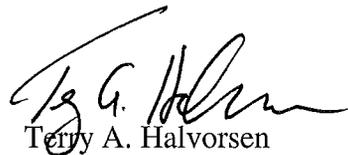
Subj: UPDATE TO DEPARTMENT OF THE NAVY APPROACH TO CLOUD COMPUTING

prior to implementation. When considering a solution that is not in the Enterprise Cloud Service Catalog and that requires a GIG connection, the requesting organization must coordinate with the Broker. The Broker will help determine if the solution should be added to the Enterprise Cloud Service Catalog or support the requesting organization governed by the GIG Waiver Process.

The DON Deputy CIO (Navy) and DON Deputy CIO (Marine Corps) will:

- Ensure all systems are properly certified and formally approved by the appropriate Designated Approval Authority, and required entries are made in the DON IT Portfolio Repository (DITPR-DON) and DON Applications and Database Management System (DADMS);
- Utilize the Broker to identify and vet commercial CSPs to host low impact systems and mission functions at lower costs than in Government owned and operated facilities;
- Analyze alternatives to identify the most cost effective hosting environment for medium impact systems, as they are defined in references (e) and (f). The analysis will evaluate commercial, Federal, and DoD solutions;
- To assist the Broker with accurately capturing requirements, categorize data as Impact levels 1-6 using the Cloud Security Model (reference h)

My point of contact for this issue is Mr. Scott Hargate, robert.hargate@navy.mil, (703) 695-2907. Additional information on Cloud Computing and the Broker can be found at <http://www.disa.mil/Services/DoD-Cloud-Broker>. Cloud Service Requests should be submitted via the Cloud Service Request portal at <http://www.disa.mil/Services/DoD-Cloud-Broker/Cloud-Service-Request>. Questions regarding the Broker should be sent to disa.meade.cae.mbx.cloud-broker@mail.mil.



Terry A. Halvorsen
Department of the Navy
Chief Information Officer

Distribution:
DISA
DUSN/DCMO
DON/AA
ASN (RD&A)
DASN C4I/Space
DON Deputy CIO (Navy)
DON Deputy CIO (Marine Corps)