



CHIEF INFORMATION OFFICER

## DEPARTMENT OF DEFENSE

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

DEC 09 2011

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: Interim Guidance Memorandum on Use of Commercial Cloud Computing Services

The Office of Management and Budget and the Federal CIO issued a Federal Cloud Computing Strategy and “25 Point Implementation Plan to Reform Federal Information Technology (IT) Management” to accelerate the pace at which the government will realize the value of cloud computing. The Department is supporting these Federal initiatives with a strategy that drives the secure and effective adoption of cloud computing to improve the resiliency and performance of our IT infrastructure. Cloud Computing and cloud services offer unprecedented opportunities for enhanced information sharing, improved mission effectiveness, and decreased costs.

Cloud computing continues to demonstrate significant benefits, but challenges remain. We must not trade the confidentiality, integrity, and interoperability of Department of Defense (DoD) information for desired benefits that may jeopardize our mission. Outsourcing DoD IT support to external cloud providers brings potential risks to the Department that must be managed at the enterprise level. The Global Information Grid (GIG) Waiver Panel, informed by the Defense Information Assurance Security Accreditation Working Group, is established to grant approval for GIG-Internet connections and derivation from existing information assurance (IA) standards. For the Department, use of third party, off-premises cloud services will require a waiver from the GIG Waiver Panel in order to preserve the security of DoD data and mission assurance in the face of persistent cyber threats from capable adversaries.

Certain commercial cloud services are maturing and showing the potential to effectively support unclassified DoD missions with low to medium assurance requirements, as demonstrated by compliance with Federal Information Security Management Act security controls. The Department’s understanding and management of the risks associated with commercially

provided cloud services are also rapidly evolving. Working with other federal agencies, the Department is supporting the Federal Risk and Authorization Management Program (FedRAMP) to establish a standard approach to assessing and authorizing cloud computing services, and to define requirements for the continuous auditing and monitoring of cloud computing providers. When implemented, the FedRAMP process will facilitate the assessment and authorization of cloud services as well as the adoption of authorized cloud services across federal agencies. In addition to supporting FedRAMP, the Department is currently revising the DoD 8500 series Issuances. Revisions include adoption of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 security controls and NIST SP 800-53a assessment procedures to enable common IA evaluation and a streamlined approval process.

An essential component of the on-going, dependable use of externally provided cloud services is the integration of a cloud provider's continuous monitoring and response capabilities with USCYBERCOM's systems for protecting DoD information and ensuring DoD mission assurance. The Department will be able to move from an approval process based on evaluation of individual waiver requests to enterprise acceptance of approved commercial cloud services once these mission assurance capabilities are implemented. With the implementation of continuous monitoring of the commercial providers, explicit definition of the roles and responsibilities for detecting and responding to cyber events, and the demonstrated ability of the DoD consumers to support their IA responsibilities, commercially offered cloud services may be approved to support DoD IT requirements.

This Memorandum serves to reinforce existing policy and processes, and is in effect for all DoD networks and systems. As FedRAMP and the DoD 8500 series issuances evolve, further guidance will follow to establish procedures for acquiring and assuring security of commercial cloud services. My point of contact for this matter is Mr. Robert Vietmeyer at email: robert.vietmeyer@osd.mil, 571-372-4461.



Teresa M. Takai