

CLLOUD COMPUTING SERVICES

- 1. REASON FOR ISSUE:** This Directive establishes the Department of Veterans Affairs (VA) policy and responsibilities regarding cloud computing services for VA.
- 2. SUMMARY OF CONTENTS/MAJOR CHANGES:** This Directive establishes policy, roles and responsibilities regarding evaluation for selection of secure cloud computing services for VA. This document also establishes VA policy for compliance with the Federal Chief Information Officer's (CIO) mandate for a 'Cloud First' policy. The CIO's policy is intended to accelerate the pace at which the government will realize the value of cloud computing by requiring agencies to evaluate safe, secure cloud computing options before making any new technology investments. This is supported by current Federal laws, Office of Management and Budget mandates, National Institute of Standards and Technology recommendations, and VA Directive and Handbook 6500, *Information Security Program*.
- 3. RESPONSIBLE OFFICE:** The Office of the Assistant Secretary for Information and Technology (005), Information Security (005R), Cyber Security (005R2) is responsible for the content contained in this Directive.
- 4. RELATED HANDBOOK:** VA Handbook 6517, *Cloud Computing Services* (under development).
- 5. RESCISSIONS:** None.

CERTIFIED BY:

/s/
Roger W. Baker
Assistant Secretary for Information and
Technology

**BY DIRECTION OF THE SECRETARY OF
VETERANS AFFAIRS:**

/s/
Roger W. Baker
Assistant Secretary for Information and
Technology

Distribution: Electronic Only

CLOUD COMPUTING SERVICES

1. PURPOSE AND SCOPE

a. The purpose of this Directive is to establish Department of Veterans Affairs (VA) policy for evaluating the use of cloud computing services within VA. This Directive establishes VA's policy to ensure compliance with Federal laws, Office of Management and Budget (OMB) mandates, National Institute of Standards and Technology (NIST) Special Publications (SP), the Federal Risk and Authorization Management Program (FedRAMP), and VA Directive and Handbook 6500, *Information Security Program*.

b. Each agency Chief Information Officer (CIO) has been directed to comply with the Federal CIO's mandated, "25 Point Implementation Plan to Reform Federal Information Technology Management," dated December 9, 2010, for the "Cloud First" initiative. This is also in compliance with the revised OMB Circular A-94, *Guidelines and Discount Rates for Benefit-Cost Analysis of Federal Programs*. The initiative requires that agency CIO's implement cloud computing services whenever possible. The Federal CIO has established FedRAMP to provide a standard approach to Assessment and Authorization (A&A) (formerly Certification & Accreditation) cloud computing services and products. The Federal CIO has directed NIST to serve as the technical advisor for assessing risks in implementation that is focused on cloud computing solutions. The assessment of risk must be consistent with the six-step Risk Management Framework identified in NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*.

c. FedRAMP is managed by the Federal CIO's Council on cloud computing and allows joint authorizations and continuous security monitoring services for government cloud computing systems intended for multi-agency use. Joint authorization of cloud providers results in a common security risk model that can be leveraged across VA in cooperation with other agencies. The use of this common security risk model provides a consistent baseline for cloud-based technologies. This common baseline ensures that the benefits of cloud-based technologies are effectively integrated across the various cloud computing solutions currently proposed within the government. There are three services that will be available for implementation. These services are the only services and platforms for implementation. The service models are: Cloud Software as a Service (SaaS); Cloud Platform as a Service (PaaS); and Cloud Infrastructure as a Service (IaaS).

d. This Directive applies to all VA organizations and information technology (IT) resources including contracted IT systems acting on behalf of VA.

2. POLICY

a. VA will comply with the requirements for a "Cloud First" policy as established by the Federal CIO. The CIO has required Agencies to evaluate the feasibility of a cloud service prior to hardware and software acquisition.

b. VA will continuously identify and evaluate available business use cases for implementation of a cloud service.

c. The VA CIO, or designee, will review and approve/disapprove cloud computing business use cases for VA. VA will ensure that NIST security requirements for cloud computing services are met.

d. VA will conduct and document a feasibility study for a cloud computing service prior to hardware and software acquisition.

e. Each prospective cloud computing business use case will be tested from a secure, approved VA facility. The testing will occur prior to adoption of the service to ensure compliance and adherence to security measures according to NIST recommendations and VA regulatory authority. This will be conducted in accordance with an A&A standardized approach for cloud computing services based on NIST "Best Practices" prior to becoming operational.

f. VA will consult with FedRAMP, as needed, to provide a standardized approach to A&A cloud computing services and products. The Federal CIO has established FedRAMP to identify requirements for cloud computing security controls and has directed NIST to serve as the technical advisor for assessing risks in implementation of these services.

3. RESPONSIBILITIES

a. **Secretary of Veterans Affairs** is responsible for designating the VA CIO as the senior agency official responsible for the Department's IT program.

b. **Assistant Secretary for Information and Technology**, as the CIO is responsible for the following:

(1) Approving cloud computing services to be used in VA;

(2) Establishing policies and procedures to ensure the provision of effective and secure cloud computing services to support the Federal CIO's mission for secure, cost-saving technological innovations to support VA's infrastructure, information systems, and data repositories;

(3) Implementing a risk management approach to IT operations that applies risk categorizations to VA information and information systems; establish secure, cost-saving procedures for implementing cloud computing services whenever feasible, and ensures a balance between risk to information systems and cost-saving cloud computing services to preserve VA business requirements and support continuity of operations;

(4) Monitoring, reviewing, and evaluating compliance with this Directive; and

(5) As the overall VA system owner, delegating the daily operations and maintenance of responsibilities to VA officials, as appropriate.

c. **Deputy CIO, Service Delivery and Engineering** is responsible for developing, procuring, integrating, modifying, maintaining, and implementation of security over VA information and information systems. Cloud computing responsibilities include:

(1) Assisting and coordinating with the VA information system owners in managing cloud computing services for VA information systems; and

(2) Assisting and coordinating with VA information system owners in creating, maintaining and submitting cloud computing service change requests for continuous monitoring, implementation, or maintenance for approval to the Enterprise Security Change Control Board (ESCCB).

d. **Deputy Assistant Secretary (DAS) for Information Security**, as VA Chief Information Security Officer, has authority over the VA enterprise cyber security budget and is responsible for ensuring that the capability of utilizing cloud computing services is properly identified and securely managed. In addition, the DAS for Information Security is responsible for:

(1) Developing VA information security policies and procedures consistent with federal laws and guidance, and VA regulations and policies;

(2) Reviewing VA information security policies and procedures related to information security that are under the management and oversight of other Department organizations;

(3) Ensuring that all Memoranda of Understanding and Interconnection Security Agreements clearly define the security controls implemented to protect the confidentiality, availability, and integrity of VA information processed, stored, or transmitted within or between interconnected systems;

(4) Ensuring voting representation on the ESCCB so that cloud computing services are executed in accordance with federal laws, OMB Circulars and Memoranda, and VA policies for privacy and records management; as well as the Federal CIO's mandated, "25 Point Implementation Plan to Reform Federal Information Technology Management" dated December 9, 2010, for the Federal Government's "Cloud First" initiative.

(5) Evaluating and testing the feasibility of cloud computing services to determine security control requirements prior to making recommendations for their adoption or refusal; and

(6) Monitoring all cloud computing services for compliance with existing federal laws and VA policies in conjunction with FedRAMP stipulations as directed by the Federal CIO Council.

e. **Under Secretaries, Assistant Secretaries, and Other Key Officials** are responsible for ensuring compliance with this Directive within their respective Administrations, Staff Organizations, and Program Offices by coordinating and collaborating with Office of Information and Technology officials.

4. TERMS AND DEFINITIONS

a. **Business use case:** Simulations are conducted on a continual basis to determine whether selected business processes are feasible for a cloud service. The business use case may be recommended for implementation once the capability for a cloud service has been determined. The business use case simulation does not include VA security controls that may be required for implementation.

b. **Cloud Infrastructure as a Service (IaaS):** The capability available to the consumer is to provide processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

c. **Cloud Platform as a Service (PaaS):** The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.

d. **Cloud Software as a Service (SaaS):** The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

5. REFERENCES

- a. 36 C.F.R. Part 1236, *Electronic Records Management*
- b. E-Government Act, P. L. 107-347, 116 Stat. 2899 (Dec 17, 2002)
- c. Federal CIO's mandated, *25 Point Implementation Plan to Reform Federal Information Technology Management*, dated December 9, 2010, for the Federal Government's "Cloud First" initiative
- d. FIPS 140-2, *Security Requirements for Cryptographic Modules*
- e. FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*
- f. FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*
- g. NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*
- h. NIST SP 800-53 rev. 3, *Recommended Security Controls for Federal Information Systems*

- i. OMB Circular A-94, *Guidelines and Discount Rates for Benefit-Cost Analysis of Federal Programs*
- j. OMB Circular A-130, *Management of Federal Information Resources*
- k. OMB Memorandum M-08-27, *Guidance for Trusted Internet Connection (TIC) Compliance*
- l. VA Directive and Handbook 6500, *Information Security Program*

ACRONYMS AND ABBREVIATIONS

- a. **A&A:** Assessment and Authorization (formerly Certification & Accreditation)
- b. **CIO:** Chief Information Officer
- c. **DAS:** Deputy Assistant Secretary
- d. **ESCCB:** Enterprise Security Change Control Board
- e. **FedRAMP:** Federal Risk and Authorization Management Program
- f. **FIPS:** Federal Information Processing Standards
- g. **IaaS:** Infrastructure as a Service
- h. **IT:** Information Technology
- i. **NIST:** National Institute of Standards and Technology
- j. **OMB:** Office of Management and Budget
- k. **PaaS:** Platform as a Service
- l. **SaaS:** Software as a Service
- m. **SP:** Special Publications
- n. **TIC:** Trusted Internet Connections
- o. **VA:** Department of Veterans Affairs