EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

December 8, 2011

MEMORANDUM FOR CHIEF INFORMATION OFFICERS

FROM: Steven VanRoekel SVR
Federal Chief Information Officer

SUBJECT: Security Authorization of Information Systems in Cloud Computing Environments

1. Introduction

Cloud computing offers a unique opportunity for the Federal Government to take advantage of cutting edge information technologies to dramatically reduce procurement and operating costs and greatly increase the efficiency and effectiveness of services provided to its citizens. Consistent with the President's International Strategy for Cyberspace and Cloud First policy, the adoption and use of information systems operated by cloud service providers (cloud services) by the Federal Government depends on security, interoperability, portability, reliability, and resiliency.

Over the past 24 months, the Administration has worked in close collaboration with the National Institute of Standards and Technology (NIST), the General Services Administration (GSA), the Department of Defense (DOD), the Department of Homeland Security (DHS), the United States Chief Information Officers Council (CIO Council) and working bodies such as the Information Security and Identity Management Committee (ISIMC), state and local governments, the private sector, non-governmental organizations (NGOs), and academia to develop the Federal Risk and Authorization Management Program (FedRAMP). This program introduces an innovative policy approach to developing trusted relationships between Executive departments and agencies[1] and cloud service providers (CSPs).

FedRAMP will provide a cost-effective, risk-based approach for the adoption and use of cloud services by making available to Executive departments and agencies:

- Standardized security requirements for the authorization and ongoing cybersecurity of cloud services for selected information system impact levels;
- A conformity assessment program capable of producing consistent independent, third-party assessments of security controls implemented by CSPs;
- Authorization packages[2] of cloud services reviewed by a Joint Authorization Board (JAB) consisting of security experts from the DHS, DOD, and GSA;

[1] References to Executive departments and agencies include all subordinate organizations within those departments and agencies.
[2] Authorization packages contain the body of evidence needed by authorizing officials to make risk-based decisions regarding the information systems providing cloud services. This includes, as a minimum, the Security Plan, Security Assessment Report, Plan of Action and Milestones and a Continuous Monitoring Plan.

- Standardized contract language to help Executive departments and agencies integrate FedRAMP requirements and best practices into acquisition; and

- A repository of authorization packages for cloud services that can be leveraged government-wide.

FedRAMP will reduce duplicative efforts, inconsistencies and cost inefficiencies associated with the current security authorization process. FedRAMP establishes a public-private partnership to promote innovation and the advancement of more secure information technologies. By using an agile and flexible framework, FedRAMP will enable the Federal Government to accelerate the adoption of cloud computing by creating transparent standards and processes for security authorizations and allowing agencies to leverage security authorizations on a government-wide scale.

2. Purpose

This memorandum:

a. Establishes Federal policy for the protection of Federal information in cloud services;

b. Describes the key components of FedRAMP and its operational capabilities;

c. Defines Executive department and agency responsibilities in developing, implementing, operating, and maintaining FedRAMP; and

d. Defines the requirements for Executive departments and agencies using FedRAMP in the acquisition of cloud services.[3]

3. Applicability

This memorandum is applicable to:

a. Executive departments and agencies procuring commercial and non-commercial cloud services that are provided by information systems that support the operations and assets of the departments and agencies, including systems provided or managed by other departments or agencies, contractors, or other sources;

b. All cloud deployment models[4] (e.g., Public Clouds, Community Clouds, Private Clouds, Hybrid Clouds) as defined by NIST;[5] and

c. All cloud service models (e.g., Infrastructure as a Service, Platform as a Service, Software as a Service) as defined by NIST.[6]

4. Roles and Responsibilities

[3] This includes Executive departments and agencies not subject to the Federal Acquisition Regulation.
[4] Executive departments or agencies that: (i) select a private cloud deployment model (i.e., the cloud environment is operated solely for the use of their organization); (ii) implement the private cloud on premise (i.e., within a Federal facility); and (iii) are not providing cloud services from the cloud-based information system to any external entities (including bureaus, components, or subordinate organizations within their agencies), are exempted from the FedRAMP requirements. In such situations, Executive departments or agencies shall continue to comply with the current FISMA requirements and the appropriate NIST security standards and guidelines for their private cloud-based information systems.
[5] This policy shall apply to all cloud deployment and service models, including any deployment/service models that are added and/or modified in future revisions to the NIST definition of cloud computing.
[6] Ibid.

This memorandum details the interaction among the four key stakeholders that make up FedRAMP: DHS, the FedRAMP JAB, a Program Management Office (PMO), and Executive departments and agencies.

a. In accordance with Office of Management and Budget (OMB) Memorandum 10-28, "*Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security*," DHS will continue to exercise primary responsibility within the Executive branch for the operational aspects of Federal agency cybersecurity with respect to the Federal information systems that fall within the Federal Information Security Management Act of 2002 (FISMA) (Title III, Pub. L. No. 107-347). Within the operational framework of FedRAMP, DHS activities will include:
    i. Assisting government-wide and agency-specific efforts to provide adequate, risk-based and cost-effective cybersecurity;
    ii. Coordinating cybersecurity operations and incident response and providing appropriate assistance;
    iii. Developing continuous monitoring standards for ongoing cybersecurity of Federal information systems to include real-time monitoring and continuously verified operating configurations;[7] and
    iv. Developing guidance on agency implementation of the Trusted Internet Connection (TIC) program with cloud services.
b. DOD, DHS, and GSA have agreed to establish a JAB and serve as permanent members of the Board. The JAB shall:
    i. Consist of Chief Information Officers from DOD, DHS, and GSA, supported by designated technical representatives from their respective member organizations;
    ii. Define and regularly update the FedRAMP security authorization requirements[8] in accordance with the Federal Information Security Management Act of 2002 (FISMA) and DHS guidance;
    iii. Approve accreditation criteria for third-party assessment organizations (3PAOs) to provide independent assessments of CSPs' implementation of the FedRAMP security authorization requirements[9];
    iv. Establish and publish priority queue requirements for authorization package reviews;
    v. Review authorization packages for cloud services based on the priority queue;

[7] DHS will work with the JAB and FedRAMP PMO to create a framework for how Executive departments and agencies can effectively and efficiently implement continuous monitoring and ongoing cybersecurity activities within FedRAMP as detailed in section 4.c.i.e.
[8] FedRAMP security authorization requirements will include a standardized baseline of security controls, privacy controls, and controls selected for continuous monitoring from NIST Special Publication 800-53 (as amended) and in accordance with accompanying NIST publications.
[9] Inspection bodies are organizations accredited to provide independent, third-party assessments of security and privacy controls based on ISO/IEC standards and technical competency criteria. Accreditation bodies are organizations that apply the ISO/IEC standards and technical competency criteria to inspection bodies to determine if those bodies have the requisite skills, expertise, and quality systems to conduct such assessments.

vi. Grant provisional authorizations for cloud services that can be used as an initial approval that Executive departments and agencies leverage in granting security authorizations and an accompanying authority to operate (ATO) for use;

vii. Ensure that provisional authorizations are reviewed and updated regularly and notify Executive departments and agencies of any changes to provisional authorizations including removal of such authorizations; and

viii. Establish methods for input to the FedRAMP security authorization requirements from all Executive departments and agencies.

c. GSA has agreed to establish a FedRAMP PMO which will:

i. Create a process for Executive departments and agencies and CSPs to adhere to the FedRAMP security authorization requirements created by the JAB to include, but not limited to:

a. A methodology for harmonizing agency-specific security and privacy controls with the FedRAMP security authorization requirements;

b. A mechanism for Executive departments and agencies and CSPs to request security authorization initiation through the FedRAMP PMO and JAB;

c. Guidance for Executive departments and agencies to satisfy FedRAMP security authorization requirements when a proposed cloud service is not prioritized for review by the FedRAMP PMO and JAB;

d. A framework for Executive departments and agencies to leverage security authorization packages processed by FedRAMP; and

e. In coordination with DHS, a framework for continuous monitoring, incident response and remediation, and FISMA reporting.

ii. Prioritize requests for authorization and authorization package review by the JAB in accordance with the JAB-approved priority queue requirements and publish and update on a continuous basis the FedRAMP priority queue;

iii. Establish a centralized, secure repository detailing requests for authorization, agency-provided authorization packages, CSP-provided authorization packages, and JAB provisional authorization packages of cloud services that Executive departments and agencies can leverage to grant security authorizations;

iv. Coordinate and collaborate with the NIST to develop and implement a formal conformity assessment program to accredit 3PAOs to provide independent assessments of how CSPs implement the FedRAMP requirements;

v. Develop and make available to Executive departments and agencies templates that can satisfy FedRAMP security authorization requirements through standard contract language and service level agreements (SLAs) for use in the acquisition of cloud services; and

vi. Develop and make available to Executive departments and agencies template Memoranda of Understanding (MOU) and/or Memoranda of Agreement (MOA) that

will govern the exchange of information between Executive departments, agencies and the FedRAMP PMO.

d. Each Executive department or agency shall:

i. Use FedRAMP when conducting risk assessments, security authorizations, and granting ATOs for all Executive department or agency use of cloud services;

ii. Use the FedRAMP PMO process and the JAB-approved FedRAMP security authorization requirements as a baseline when initiating, reviewing, granting and revoking security authorizations for cloud services;[10]

iii. Ensure applicable contracts appropriately require CSPs to comply with FedRAMP security authorization requirements;

iv. Establish and implement an incident response and mitigation capability for security and privacy incidents for cloud services in accordance with DHS guidance;

v. Ensure that acquisition requirements address maintaining FedRAMP security authorization requirements and that relevant contract provisions related to contractor reviews and inspections are included for CSPs;

vi. Consistent with DHS guidance, require that CSPs route their traffic such that the service meets the requirements of the Trusted Internet Connection (TIC) program; and

vii. Provide to the Federal Chief Information Officer (CIO) annually on April 30, a certification in writing from the Executive department or agency CIO and Chief Financial Officer, a listing of all cloud services that an agency determines cannot meet the FedRAMP security authorization requirements with appropriate rationale and proposed resolutions.

e. The CIO Council shall publish and disseminate information from the FedRAMP PMO and JAB to Executive departments and agencies.

5. FedRAMP Operational Capability

a. Within 30 days of the issuance of this policy, the CIO Council will publish the standardized baseline of security controls, privacy controls, and controls selected for continuous monitoring from NIST Special Publication 800-53 (as amended) included within the FedRAMP security authorization requirements;

b. Within 60 days of the issuance of this policy, the FedRAMP PMO shall publish a Concept of Operations (CONOPS) for FedRAMP providing the initial process for Executive departments and agencies and CSPs to adhere to the FedRAMP security authorization requirements created by the JAB. The CONOPS shall be updated, as required, by the FedRAMP PMO and made available to Executive departments and agencies and CSPs;

c. Within 90 days of the issuance of this policy, the JAB shall publish a charter which defines its governance model; and

[10] For all currently implemented cloud services or those services currently in the acquisition process prior to FedRAMP being declared operational, security authorizations must meet the FedRAMP security authorization requirement within 2 years of FedRAMP being declared operational.

d. Within 180 days of the issuance of this policy, the FedRAMP PMO will provide an initial operating capability for FedRAMP.

6. Effects and Compliance with Existing Federal Laws, Directives, and Policies

Nothing in this memorandum shall be construed to supersede existing Executive department and agency responsibilities for complying with information security and privacy requirements defined by existing Federal laws, Executive Orders, directives, standards, guidelines, or regulations.

7. References

a. Federal Information Security Management Act (P.L. 107-347, Title III), December 2002.

b. Office of Management and Budget, Circular A-130, Appendix III, Transmittal Memorandum #4, *Management of Federal Information Resources*, November 2000.

c. NIST Federal Information Processing Standards Publication 199 (as amended), *Standards for Security Categorization of Federal Information and Information Systems*.

d. NIST Federal Information Processing Standards Publication 200 (as amended), *Minimum Security Requirements for Federal Information and Information Systems*.

e. NIST Special Publication 800-18 (as amended), *Guide for Developing Security Plans for Federal Information Systems*.

f. NIST Special Publication 800-30 (as amended), *Guide for Conducting Risk Assessments*, (Projected Publication 2011).

g. NIST Special Publication 800-37 (as amended), *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*.

h. NIST Special Publication 800-39 (as amended), *Managing Information Security Risk: Organization, Mission, and Information System View*.

i. NIST Special Publication 800-53 (as amended), *Recommended Security Controls for Federal Information Systems and Organizations*.

j. NIST Special Publication 800-53A (as amended), *Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans*.

k. NIST Special Publication 800-60 (as amended), *Guide for Mapping Types of Information and Information Systems to Security Categories*.

l. NIST Special Publication 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*.

m. NIST Special Publication 144 (Draft), *Guidelines on Security and Privacy in Public Cloud Computing*.

n. NIST Special Publication 145, *A NIST Definition of Cloud Computing*.

o. ISO/IEC 17011: Conformity Assessment – General requirements for accreditation bodies accrediting conformity assessment bodies.

p. ISO/IEC 17020: General criteria for the operation of various types of bodies performing inspection.

q. The Office of Management and Budget, *The Federal Cloud Computing Strategy*.

Any questions regarding this memorandum should be directed to FedRAMP@omb.eop.gov.