Federal Risk and Authorization Management Program Joint Authorization Board Charter

Version 1.0

February 28, 2012

Document History

Document Location

This is a snapshot of an on-line document. Paper copies are valid only on the day they are printed. The source of the document will be maintained on FedRAMP.gov.

Revision History

Version	Revision Date	Summary of Changes	Changes by
V0.1		Preliminary Draft	FedRAMP PMO
V0.2	11/02/2011	Changes per OMB Policy Memo	FedRAMP PMO

Approvals

The following approvals are required for this document:

27 February 2012

Ms. Casey Coleman, CIO, GSA
Date:

Mr. Richard Spires, CIO, DHS
Date: 2/27/2012

Teri Takai

Ms. Teri Takai, CIO, DOD
Date:

Table of Contents

I. Purpose

The purpose of this Charter is to define the authority, objectives, membership, roles and responsibilities, meeting schedule, decision making requirements, and establishment of committees for the Federal Risk and Authorization Management Program (FedRAMP) Joint Authorization Board (JAB) in accordance with OMB Memo *"Security Authorizations of Information Systems in Cloud Computing Environments"* (hereinafter referred to as FedRAMP Policy Memo).

II. Background

The White House has worked in close collaboration with the National Institute of Standards and Technology (NIST), General Services Administration (GSA), Department of Defense (DOD), Department of Homeland Security (DHS), Federal Government Chief Information Officers Council (CIOC) and working bodies such as the Information Security and Identity Management Committee (ISIMC), state and local Governments, the private sector, non-governmental organizations (NGO), and academia to develop the Federal Risk and Authorization Management Program (FedRAMP).

As a part of this program, the Chief Information Officers of DHS, DOD, and GSA, at the direction of the Federal CIO, have agreed to establish a Joint Authorization Board (JAB). The JAB will provide the technical knowledge and skills to provide a government-wide baseline approach to address the security needs associated with placing Federal data in cloud computing solutions. Additionally, the JAB will provide joint provisional[1] security authorizations of cloud solutions using this baseline approach. This provisional authorization will create an authorization package that can be leveraged by individual agencies across the Federal Government to grant an Authority to Operate at their respective organizations.

III. Authority

The authority of the FedRAMP JAB comes from the FedRAMP Memo.

IV. Objectives

In accordance with the FedRAMP Memo the following objectives have been outlined for the JAB:

1) Define and regularly update FedRAMP security authorization requirements in accordance with the Federal Information Security Management Act of 2002 (FISMA) and DHS guidance;
   a) 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.
   b) The JAB will work with DHS National Protection and Programs Directorate (NPPD) to further develop continuous monitoring standards to include near-real time monitoring and continuously verified operating configurations as well as coordinated incident response and threat notification.

[1] A provisional authorization is an initial statement of risk and approval of an authorization package by the JAB pending the issuance of a final authorization to operate by the Executive department or agency acquiring the cloud service.

   c) FedRAMP security authorization requirements will require review by qualified third party assessment organization (3PAO) to independently verify and validate the implementation of these controls on a Cloud Service Provider (CSP) environment.

2) Approve accreditation criteria for third party assessment organizations (3PAOs) to provide independent assessments of cloud service providers' implementation of the FedRAMP security authorization requirements;
   a) The JAB will approve the criteria necessary to qualify 3PAOs according to:
      i) Independence and quality management specifications based on ISO/IEC standards to ensure the requisite independence and quality systems needed to assess the security control implementations by CSPs; and
      ii) Technical competency criteria based on an evaluation of knowledge of security authorizations to ensure the requisite skills and expertise to conduct such assessments.
   b) The JAB will regularly review the accreditation criteria; and
   c) Per FedRAMP Policy Memo, the JAB will provide the accreditation criteria to approve 3PAOs to the FedRAMP PMO in order for the FedRAMP PMO to implement a conformity assessment program to qualify and approve 3PAOs.

3) Establish and publish priority queue requirements for authorization package reviews;
   a) The JAB will publish the priority queue requirements on FedRAMP.gov to ensure transparency;
   b) The JAB will regularly review the priority queue requirements and update as needed to ensure these requirements ensure maximum government-wide leveraging of FedRAMP provisional authorization packages; and
   c) Per FedRAMP Policy Memo, the JAB will provide the priority queue requirements to the FedRAMP PMO to prioritize cloud systems for JAB review.

4) Review authorization packages for cloud services based on the priority queue;
   a) The JAB will review authorization packages provided by the FedRAMP PMO on a rolling basis and in a timely manner as resources allow.

5) Grant provisional authorizations for cloud services that Executive departments/agencies can use as an initial approval in granting security authorizations and an accompanying authority to operate (ATO) for use;
   a) The JAB will grant provisional authorizations by evaluating authorization packages, 3PAO results and FedRAMP PMO input.
   b) The JAB may or may not issue a provisional authorization based on the overall evaluation of artifacts provided and the resulting determination of the risk level of a CSP environment.
   c) Provisional authorization may include additional risk statements or conditions based on review of materials

6) Ensure that provisional authorizations are reviewed and updated regularly and work with the FedRAMP PMO to notify Executive departments/agencies of any changes to provisional authorizations including removal of such authorizations; and

7) Establish methods for input to the FedRAMP security authorization requirements from all Executive departments and agencies.
   a) The JAB will at a minimum invite all Executive department and agency CIOs to one JAB meeting a year to provide input to the FedRAMP security authorization requirements.

b) The JAB will work with the FedRAMP PMO to establish methods for regular input by Executive departments and agencies to ensure the FedRAMP security authorization requirements are meeting the needs of the Federal government.

V. Membership

The following reflects FedRAMP roles and membership as they pertain to the JAB:

Role	Membership
JAB Authorizing Officials	• Department of Defense (DOD) CIO • Department of Homeland Security (DHS) CIO • General Services Administration (GSA) CIO
JAB Technical Representatives	• Designee(s) of DOD CIO • Designee(s) of DHS CIO • Designee(s) of GSA CIO
FedRAMP PMO	• The FedRAMP PMO is an administrative and technical support team operating under the guidance of GSA within the Office of Citizen Services and Innovative Technologies.

VI. Roles and Responsibilities

The following describes the general and specific duties expected of each role in support.

Role	Duties and Responsibilities
JAB Authorizing Officials	• Designate JAB Technical Representative(s) • Issue joint provisional authorization decisions • Resolve issues as needed • Define FedRAMP security authorization requirements
JAB Technical Representatives	• Provide subject matter expertise to implement the direction of the respective JAB Member • Support the FedRAMP office in defining and implementing the joint provisional authorization process • Provide assessments of FedRAMP authorization packages • Recommend provisional authorization decisions based on their assessments to the respective JAB Members • Escalate issues to the respective JAB Members as appropriate
FedRAMP PMO	• Work with the JAB to create a process and framework for Federal agencies to meet FedRAMP requirements • Facilitate the provisional authorization process with CSPs and Federal agencies to include administrative and technical resources to ensure quality and complete authorization packages are provided for assessments by the JAB and the respective technical representatives • Implement a conformity assessment program to qualify and approve 3PAOs according to the criteria approved by the JAB • Prioritize JAB review of cloud systems according to the priority queue requirements approved by the JAB

Role	Duties and Responsibilities
	• Conduct outreach and education on FedRAMP with stakeholders, including federal agencies, industry and oversight organizations.

VII. Meetings

1) JAB Authorizing Officials will:
   a) Meet formally in person, at a minimum, twice per year; and
   b) Meet informally as required to make decisions in light of issues raised by the JAB technical representatives and discuss any updates needed to address new risks, threats or requirement.

2) The JAB technical representatives will:
   a) Meet, at a minimum, on a monthly basis; and
   b) Meet more regularly as required based on new risks, threats or requirements.

3) The FedRAMP PMO will:
   a) Organize, schedule and prepare agendas and minutes for all meetings as needed.

VIII. Decision Making

1) All FedRAMP JAB decisions must be agreed to by a majority of the JAB Authorizing Officials (or as designated to a respective Deputy CIO as needed) for decisions affecting:
   a) Security authorization requirements (section IV(1));
   b) 3PAO criteria (section IV(2));
   c) Priority queue requirements (section IV(3));
   d) Provisional authorization reviews and updates (section IV(6)); and
   e) Methods for input to security authorization requirements (section IV(7)).

2) All FedRAMP JAB decisions must be agreed to unanimously by all JAB Authorizing Officials (or as designated to a respective Deputy CIO as needed) for decisions affecting provisional authorizations.

IX. Committees

The JAB may establish standing councils and working groups as necessary to consider items of concern to the Joint Authorization Board.

X. Charter Review

This Charter will be reviewed on at least an annual basis to evaluate its effectiveness and incorporate any improvements. Changes to the Charter must be approved by consensus among all JAB Authorizing Officials.