FedRAMP Update
Information Security and Privacy Advisory Board

Kathy Conrad
Principal Deputy Associate Administrator
Office of Citizen Services and Innovative Technologies
October 12, 2012

GSA

FedRAMP SM

FedRAMP Progress: Since June 2012 Launch

- Over 50 applications for JAB provisional ATO submitted by Cloud Service Providers – 6 in active review; all contacted by PMO to assess readiness
- Joint Authorization Board prioritized CSPs for provisional authorization based several factors including:
  - Acquisition Ease – (Secure IaaS BPA Holder, Government Wide Commodity Vehicle, Shared Service)
  - Cross Government Readiness
  - Broad-based Solution Diversity
  - FISMA Readiness and Assessor readiness
  - Agency Demand
- Identified over 80 opportunities where ATOs can be leveraged
- Secure repository established in MAX allows CSPs to upload documents for review and agencies to access security assessment packages
- 15 accredited 3PAOs – rolling acceptance

FedRAMP Phases and Timeline

Phased evolution towards sustainable operations allows for the management of risks, capture of lessons learned, and incremental rollout of capabilities

		FY12	FY13 Q2	FY14
	Pre-	**Initial Operational Capabilities (IOC)**	**Full Operations**	**Sustaining Operations**
	Finalize … Documentation in Preparation of Launch	*Launch IOC with Limited Scope and Cloud Service Provider (CSP)s*	*Execute Full Operational Capabilities with Manual Processes*	*Move to Full Implementation with On-Demand Scalability*
Key Activities	• Publish FedRAMP Requirements (Security Controls, Templates, Guidance) • Publish Agency Compliance Guidance • Accredit 3PAOs • Establish Priority Queue	• Authorize CSPs • Update CONOPS, Continuous Monitoring Requirements and CSP Guidance	• Conduct Assessments & Authorizations • Scale Operations to Authorize More CSPs	• Implement Electronic Authorization Repository • Scale to Steady State Operations
Outcomes	• Initial List of Accredited 3PAOs • Launch FedRAMP into Initial Operating Capabilities	• Initial CSP Authorizations • Established Performance Benchmark	• Multiple CSP Authorizations • Defined Business Model • Measure Benchmarks	• Authorizations Scale by Demand • Implement Business Model • Self-Sustaining Funding Model Covering Operations • Privatized Accreditation Board

We Are Here!

Gather Feedback and Incorporate Lessons Learned

Our Commitment During IOC

- Issue three FedRAMP Provisional Authorizations by the end of 2012
- Build out the FedRAMP repository with cloud computing security assessment packages that meet FedRAMP requirements
- Actively update the program's processes and procedures during IOC in preparation for full operations
- Keep all stakeholders informed

Remaining Challenges

- All assessments of cloud-based products and services must meet FedRAMP security requirements:
  - Use baseline set of controls and templates
  - Deposit documents in secure repository
- Not all cloud products and services are required to get a JAB provisional ATO; Several “paths” to complying with FedRAMP :
  - JAB signed provisional ATO
  - Agency granted ATO
  - CSP initiated request to FedRAMP for ATO
- Agencies must start their ATO process with a query to the FedRAMP repository for existing security packages
- Still addressing challenges – e.g. working on solutions for complying with background investigation requirement

FedRAMP Repository

FedRAMP PMO maintains a repository of standardized security assessment packages that Federal Agencies can leverage to make their own risk-based decisions to grant an Authority to Operate for a cloud solution for their Agency.

The repository is key to the "do once, use many times" approach

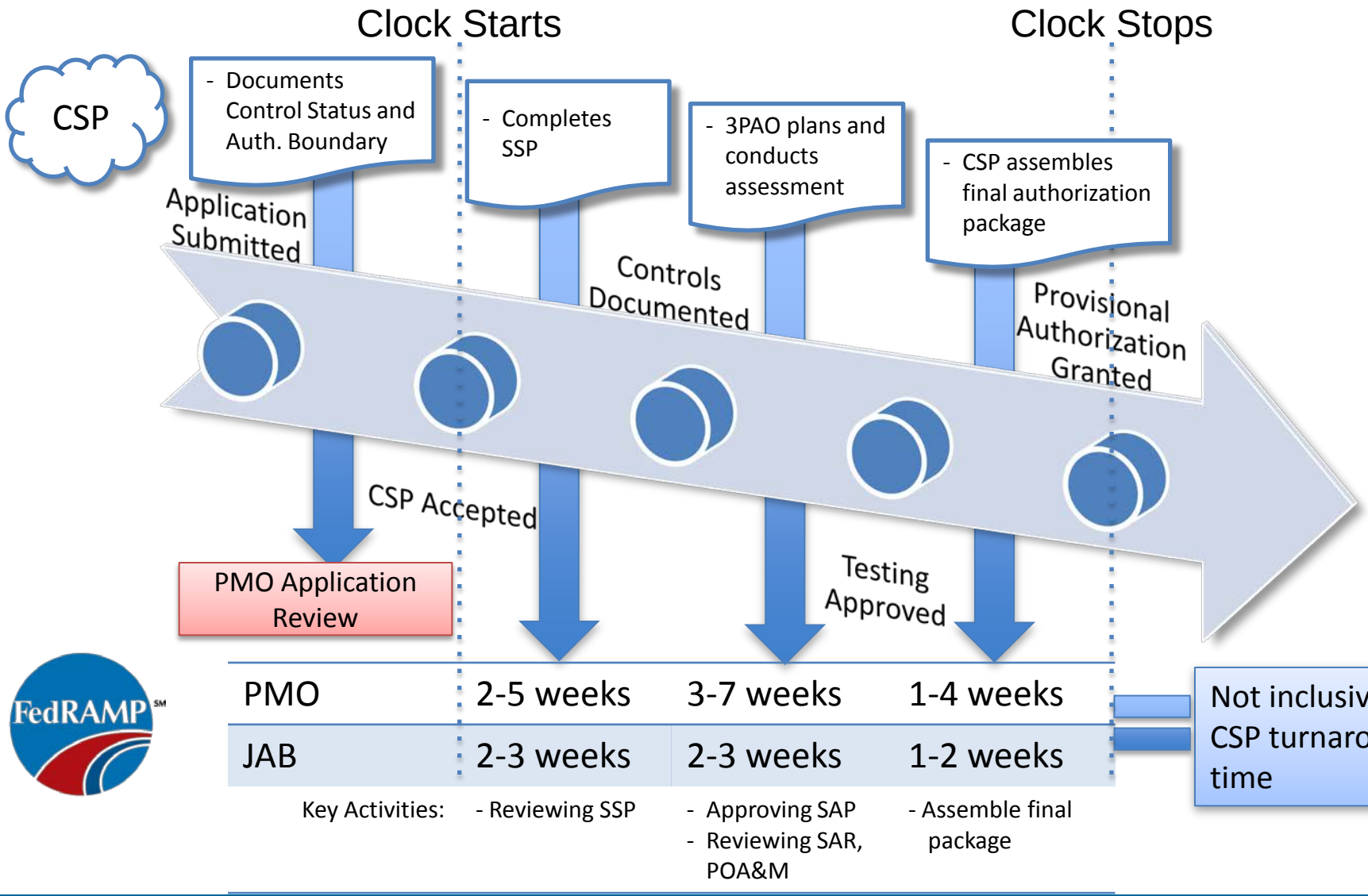
Per OMB policy memo, all assessment packages must use the FedRAMP security requirements – which includes the FedRAMP baseline set of controls as well as all FedRAMP templates

Category	FedRAMP 3PAO	ATO Status
JAB Provisional Authorization	✓	JAB (+Agency)
Agency ATO with FedRAMP 3PAO	✓	Agency
Agency ATO**	✗	Agency
CSP Supplied	✓	n/a

Level of Gov't Review

*** A&A packages without a FedRAMP 3PAO do not meet the independence requirements created by the JAB and are not eligible for JAB review*

FedRAMP Provisional Authorization Timeline - Reviews can be conducted in parallel



Readiness and Leveraging

- Interviewing all CSP applicants to assess readiness – see checklist
- Conduct quality check on system security plan – if warranted
  - Less than 20% of applicants are deemed ready to go
  - Many CSPs need education on required documentation and appropriate level of detail
- Success of the program depends on quality and completeness of security implementation packages and rigorous, but practical risk review
- Agencies are required to deposit their ATO packages in secure repository so they can be leveraged across government
  - First package in the queue
  - Strong interest from agencies to leverage
- Strong demand – identified over 80 opportunities for cloud computing that could leverage FedRAMP ATOs based on response to survey of agencies and CSPs

Before you begin… the *checklist for CSPs*

Checklist		Description
☐	1	You can process electronic discovery and litigation holds
☐	2	You can clearly define and describe your system boundaries
☐	3	You can identify customer responsibilities and what they must do to implement controls
☐	4	System provides identification & 2-factor authentication for network access to privileged accounts
☐	5	System provides identification & 2-factor authentication for network access to non-privileged accounts
☐	6	System provides identification & 2-factor authentication for local access to privileged accounts
☐	7	You can perform code analysis scans for code written in-house (non-COTS products)
☐	8	You have boundary protections with logical and physical isolation of assets
☐	9	You can remediate high risk issues within 30 days, medium risk within 90 days
☐	10	You can provide an inventory and configuration build standards for all devices
☐	11	System has safeguards to prevent unauthorized information transfer via shared resources
☐	12	Cryptographic safeguards preserve confidentiality and integrity of data during transmission

Lessons Learned

- FedRAMP is not a linear program, it operates on parallel workflows to gain efficiencies
  - Requesting CSPs submit SSP in parallel to the Tailoring Workbook and Implementation Summary
  - Assessing CSP readiness up front based on SSP and responses to checklist
- Potential for leverage needs to be balanced with CSP readiness
- Constant and consistent contact between the ISSOs and CSP key to getting approvals and maintaining schedule
- Instructions and definitions have been clarified based on feedback

Success Depends on All Partners

Agencies:

- Conduct quality risk assessments that can be leveraged
- Accept the FedRAMP ATO as the baseline for their risk assessments
- Deposit ATO documents in the repository

CSPs

- Submit quality documentation in support of their FedRAMP application
- Encourage customers to leverage existing ATOs for their products

3PAOs

- Maintain independence as part of the quality assurance process

FedRAMP PMO

- Provide an integrous process and efficient review schedule
- Support CSPs and agencies through the process
- Maintain security repository of FedRAMP ATOs

GSA

For more information, please contact us or visit us at any of the following websites:

http://FedRAMP.gov
http://gsa.gov/FedRAMP
Follow us on twitter @ FederalCloud