Federal Risk and Authorization Management Program (FedRAMP)

David L. McClure, Ph.D.
Associate Administrator
Citizen Services & Innovative Technologies

Briefing for the Information Security and Privacy Advisory Board
February 14, 2013
FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

Our approach uses a “do once, use many times” framework designed to save cost, time, and staff required to conduct redundant agency security assessments.
FedRAMP Key Benefits

• Increases re-use of existing security assessments across agencies
• Saves significant cost, time and resources – do once, use many times
• Improves real-time security visibility
• Supports risk-based security management
• Provides transparency between government and cloud service providers (CSPs)
• Improves trustworthiness, reliability, consistency, and quality of the Federal security authorization process
FedRAMP and the Security Assessment and Authorization Process

FedRAMP
Program Management Office and Joint Authorization Board

- Maintains Security Baseline including Controls & Continuous Monitoring Requirements
- Maintains Assessment Criteria
- Maintains Active Inventory of Approved Systems

Ongoing A&A (Continuous Monitoring)
Continuous Review of Risk
- Oversight of the Cloud Service Provider’s ongoing assessment and authorization activities with a focus on automation.

Assessment
- Independent Assessment
  - Before granting a provisional authorization, Cloud Service Provider systems must be assessed by an approved, Independent Third Party Assessment Organization

Authorizations:
1. Provisional ATO - Joint Authorization Board
2. ATO – Individual Agencies
3. Cloud Service Provider supplied packages

Provisional Authorization
Grant Provisional Authorization
- Joint Authorization Board reviews assessment packages and grants provisional authorizations
- Agencies issue ATOs using a risk-based framework

Independent Assessors to be retained from FedRAMP approved list of 3PAOs

Consistency and Quality

Trustworthy & Re-useable

Ongoing Assurance

Ongoing A&A Activities Will Be Coordinated Through:
1. DHS – US CERT Incident Response and Threat Notifications
2. FedRAMP PMO – POA&Ms, Scan Reviews, and ongoing assessment
### FedRAMP Phases and Timeline

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

<table>
<thead>
<tr>
<th>FY12</th>
<th>FY12</th>
<th>FY13 Q3</th>
<th>FY14</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Pre-Launch Activities</strong></td>
<td><strong>Initial Operational Capabilities (IOC)</strong></td>
<td><strong>Full Operations</strong></td>
<td><strong>Sustaining Operations</strong></td>
</tr>
<tr>
<td>Finalize Requirements and Documentation in Preparation of Launch</td>
<td>Launch IOC with Limited Scope and Cloud Service Provider (CSP)s</td>
<td>Execute Full Operational Capabilities with Manual Processes</td>
<td>Move to Full Implementation with On-Demand Scalability</td>
</tr>
</tbody>
</table>

#### 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

Gather Feedback and Incorporate Lessons Learned
FedRAMP Accomplishments since June 6, 2012

**Cloud Service Providers**
- Over 80 Applicants
- Two 2 Provisional Authorizations (Autonomic Resources, CGI)

**3PAOs**
- Over 50 Applicants
- 16 Accredited 3PAOs

**FedRAMP Program Office**
- Published Baseline, Templates and Guidance
- Secure repository used by CSPs and storing FedRAMP Security Assessment Packages
- ISSOs engaged with prioritized CSPs
- Over 7500 touch points with industry, agencies

**Federal Agencies**
- Engagement with agencies granting “Agency ATOs”
- Multiple agencies reviewing documentation
### FedRAMP Applicant Providers Overview

<table>
<thead>
<tr>
<th>Deployment</th>
<th>IaaS</th>
<th>PaaS</th>
<th>SaaS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public Cloud</td>
<td>• Virtual Machines</td>
<td>• .Net Code</td>
<td>• CRM</td>
</tr>
<tr>
<td></td>
<td>• Storage</td>
<td>• Java Code</td>
<td>• BPM</td>
</tr>
<tr>
<td></td>
<td>• CDN</td>
<td></td>
<td>• Collaboration</td>
</tr>
<tr>
<td></td>
<td>• VDI</td>
<td></td>
<td>• Software Security Testing</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Finance</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Travel</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Proj. Mgmt.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Human Resource</td>
</tr>
<tr>
<td>Private Cloud</td>
<td>• Virtual Machines</td>
<td>• Web Hosting</td>
<td>• BPM</td>
</tr>
<tr>
<td></td>
<td>• Storage</td>
<td></td>
<td>• Human Resource</td>
</tr>
<tr>
<td></td>
<td>• VDI</td>
<td></td>
<td>• FOIA</td>
</tr>
<tr>
<td></td>
<td>• Cloud Backup</td>
<td></td>
<td>• Acquisition Mgmt.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Online Training</td>
</tr>
<tr>
<td>Gov. Community Cloud</td>
<td>• Virtual Machines</td>
<td>• Web Hosting</td>
<td>• Access Control</td>
</tr>
<tr>
<td></td>
<td>• Storage</td>
<td></td>
<td>• Human Resource</td>
</tr>
<tr>
<td></td>
<td>• VDI</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hybrid Cloud</td>
<td>• Virtual Machines</td>
<td>• Web Hosting</td>
<td>• Acquisition Mgmt.</td>
</tr>
<tr>
<td></td>
<td>• Storage</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*80+ Applicants*
Privacy and PII Concerns in the Cloud

- Privacy concerns in the cloud relate to both preventing and reacting to PII incidents

- FedRAMP reviews prevention measures in technical implementation:
  - Tenant isolation, boundary protection
  - Effective separation from corporate networks
  - Data sanitization of media for in-motion activities (i.e. VM de-provisioning)
  - Proper identity proofing mechanisms and secure communications

- Management and Operational controls are also key:
  - Are policies in place to allow proper response and provide transparency?
  - Do incident response procedures for alignment with NIST processes?
  - Does the CSP have the US-CERT notification processes in place?

- No substitute for effective contractual measures during acquisition
  - Establish SLAs upfront with penalties for non-performance
  - Understand the relationship between reseller and CSP
  - Document communication processes for incident responses
FedRAMP Privacy Approach

• FedRAMP requires all providers to complete a Privacy Threshold Analysis (PTA)
  *(PTA template available on fedramp.gov)*

• If CSP is storing PII, the 3PAO completes a Privacy Impact Assessment including:
  – Rationale for collection, Attributes of collection
  – Sources and storage durations
  – Access control, Safeguards
  – Contracts, Agreements and Ownership
  – Management, Maintenance and Business Processes

• CSP’s Privacy Officer is required to sign off on the process

• This information is vetted by the JAB and available to every leveraging agency as part of the package
Lessons Learned

• Level of effort for thoroughly addressing all security controls in FedRAMP baseline is greater than expected
  – Vendors need sufficient time to adequately document their security implementations
  – FedRAMP has very rigorous standards for documentation due to government-wide nature of the authorizations
  – Expect greater efficiency as industry and government gain experience

• Prioritizing highest impact issues in the review process
  – Encryption standards (FIPS 140-2)
  – Multi-Factor Authentication
  – Appliances outside of direct CSP control (e.g. databases, authentication devices)
  – Boundaries

• Program improvements to increase time efficiencies:
  – Enhanced readiness reviews with CSPs
  – Parallel reviews of documentation
  – Reducing number of documents required get approval for testing

• JAB Agency reviews gaining efficiency as FedRAMP team better aligns expectations among stakeholders
Continuous Monitoring – the Next Frontier

- FedRAMP now monitoring providers with Provisional Authorizations
- Periodic assessment activities defined in FedRAMP’s Continuous Monitoring Strategy & Guide (on fedramp.gov)
- FedRAMP’s current strategy involves monthly reviews of key activities (POA&M, scan reports)
- Applying the Configuration Management processes as authorized Cloud Providers are growing and enhancing offerings
- Leveraging Agencies will benefit from these processes
- Working with DHS to evolve the monitoring process into a sustainable process that provides better situational awareness
Upcoming Program Developments

• Revision of Baseline
  – NIST will be updating the 800-53 control requirements from version 3 to version 4
  – Additional controls will specifically address privacy concerns
  – FedRAMP will have a public comment period to align baseline with new requirements
  – Expect updated baseline approximately 6 months after NIST finalizes revision 4
  – Update will occur within timeframe NIST gives agencies to move to the new standard (usually 1 year)

• Inclusion of High watermark in FedRAMP baselines
  – JAB does not think industry and government are ready for high baseline
  – DHS and DOD are working with CNSS to define high requirements and will work with FedRAMP as CNSS finalizes

• Privatization of 3PAO Accreditation
  – In coordination with NIST to move accreditation from a government review board (comprised of NIST and GSA) to a private review board
  – NIST has done similar efforts with health IT, common criteria labs, Underwriter’s Labs (UL) and others.
Key Take Aways

- Launched on June 6, 2012; initial operating capability
  - Successfully proving that authorization process works

- Processes address lessons learned from previous efforts
  - Provide in-depth support for each CSP
  - Authorization process based on multi-stage approvals

- Response from CSPs and 3PAOs encouraging – robust applications, high level of interest from community

- Initial Operating Capability allows testing and vetting of processes, templates, and communications

- Ongoing communication and transparency will continue to be critical to success
For more information, please contact us or visit us at any of the following websites:

http://FedRAMP.gov
info@fedramp.gov

Follow us on twitter @ FederalCloud