Using FedRAMP to Enable Secure Cloud Computing

Chris Hoover, CISA, CISSP
Thursday, January 31, 2013
Disclaimer – Safe Harbor Statement

• This presentation is for informational purposes only. This document contains certain statements that may be deemed “forward-looking statements" within the meaning of the Private Securities Litigation Reform Act of 1995.

• Forward-looking statements are based on assumptions and assessments made by us in light of our experience and perception of historical trends, current conditions and expected future developments. Actual results and timing of events may differ materially from those contemplated by the forward-looking statements due to a number of factors, including regional, national or global political, economic, business, competitive, market and regulatory conditions.

• Any reproduction, retransmission, or republication of all or part of this document is expressly prohibited without the permission of RSA.
Introduction

• Chris Hoover, RSA Archer Federal Solution Manager
• 15 years in federal IA
• Majority of this time in C&A/A&A methodologies: DITSCAP, DIACAP, NISPOM, DODIIS, DCID 6/3, and NIST RMF
• Hired by Archer to “federalize” their offerings
• Just finished demo environment of C&A/A&A tool and CM tool

• FedRAMP is, after all, just another A&A methodology
Before We Start...

• FedRAMP is brand new
  – Only 1 provisional ATO so far!

• Processes are still being refined and will change

• I do not speak for GSA, the FedRAMP JAB, etc.
Agenda

• Background of FCCI and FedRAMP
• How FedRAMP works
• Compare/contrast with NIST RMF
• How does Archer fit in?
• Questions
Why the Cloud?

• The Federal Cloud Computing Initiative’s (FCCI) mission is to drive the adoption of cloud computing solutions in the federal government and to address obstacles to that adoption.

• Benefits:
  – pay only for the resources used in response to high and low demand
  – avoid expenses of building and maintaining an IT infrastructure
Why the Cloud?

• centralize security administration

• cloud computing is essential for achieving & enabling data center consolidation, an area identified as a key federal priority ($20B /year!).

• will enable the closure* of estimated 962 federal data centers by 2015

* - through consolidation, no net loss of service
Why the Cloud? (the bottom line)

• Ensure that cloud based services used government-wide have adequate information security

• cheaper
• cheaper
• cheaper
• cheaper
• cheaper
What is FedRAMP?

• Federal Risk and Authorization Management Program

• A&A/CM scheme for cloud based systems / cloud environments

• methodology based on NIST RMF
What is FedRAMP?

FedRAMP is the Federal Risk and Authorization Management Program, a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. The program is managed by the National Institute of Standards and Technology (NIST) and operated by the National Security Agency (NSA) and the Department of Homeland Security (DHS).

www.fedramp.gov
Who is Involved?

- GSA – PMO, purchasing, FCCI
- NIST – NIST RMF, SP 800 - series library
- DoD – size, history
- DHS - .gov oversight, CM initiatives
- Blue = JAB
Why FedRAMP?

• Many similar benefits of cloud: “do once, use many”
• Similar to normal A&A concepts of inheritance / common controls
• Most-all controls will be satisfied by the host environment
• Little to no A&A burden on the customer agency
Why FedRAMP?

• Before: every agency pays for the A&A for every system they own separately

• After: the vendor pays for the A&A of the cloud environment once and all the customer agencies benefit
FedRAMP Terms and Concepts

• CSP – Cloud Service Provider
• 3PAO – Third Party Assessment Org
• JAB – Joint Authorization Board
• Provisional ATO
Cloud Service Provider (CSP)

• The vendor trying to sell cloud services to the federal customer

• Has the burden of implementing security and doing most/all of A&A compliance activities

• In traditional A&A terms would be filling the roles of both an Information System Owner and a Common Control Provider
Cloud Service Provider (CSP)

Authorized CSPs

CSP Name: Autonomic Resources LLC

Service Name: ARC Platform (ARC-P) system

Description: Autonomic Resources provides the capability for the customer to provision processing, storage, networks, and other fundamental computing resources upon which the customer is able to deploy and run operating systems and applications through Virtual Machines.

Service Model: Infrastructure as a Service (IaaS)

ATO/Submission Date: 12/26/2012

Repository Level: JAB Provisional Authorization

Deployment Model: Government Community

3PAO: Veris Group (FedRAMP accredited)

If you are a federal agency wishing to leverage this authorization, please send an email request to the FedRAMP PMO at info@FedRAMP.gov with the message subject “Leverage Authorization.”
Third Party Assessment Organizations (3PAOs)
Third Party Assessment Organizations (3PAOs)

- Fills the role of what would normally be an SCA
- Some 3PAOs offering (phase 1) support, filling out authorization package artifacts – if they do, they can not do control assessment
- Develop assessment plan, perform assessments, and deliver SAR
- Assessment results they provide are used by JAB to make authorization decision
Third Party Assessment Organizations (3PAOs)

• The FedRAMP PMO accredits 3PAOs

• It is not a hard requirement to use official FedRAMP assessor, but if you don’t, you have additional burden of showing qualifications for the assessor

• 3PAO qualifications are based in large part on NIST-based conformity testing

• Conformity testing tests independence, technical competence, and promotes conformity in FedRAMP assessments
## Third Party Assessment Organizations (3PAOs)

<table>
<thead>
<tr>
<th>Organization</th>
<th>POC Name</th>
<th>POC Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>BrightLine</td>
<td>Doug Barbin</td>
<td><a href="mailto:3PAO@brightline.com">3PAO@brightline.com</a></td>
</tr>
<tr>
<td>COACT, Inc.</td>
<td>Brian Pleffner</td>
<td><a href="mailto:bpleffner@coact.com">bpleffner@coact.com</a></td>
</tr>
<tr>
<td>Coalfire Systems</td>
<td>Tom McAndrew</td>
<td><a href="mailto:3PAO@coalfire.com">3PAO@coalfire.com</a></td>
</tr>
<tr>
<td>Department of Transportation (DOT)</td>
<td>Jerome Kemp</td>
<td><a href="mailto:IT_Security_Services@esc.gov">IT_Security_Services@esc.gov</a></td>
</tr>
<tr>
<td>Enterprise Services Center (ESC)</td>
<td>Prenston Gale</td>
<td><a href="mailto:3PAO@drc.com">3PAO@drc.com</a></td>
</tr>
<tr>
<td>Dynamics Research Corporation (DRC)</td>
<td>Yusuf Ahmed</td>
<td><a href="mailto:yaa@earthlingsecurity.com">yaa@earthlingsecurity.com</a></td>
</tr>
<tr>
<td>Earthling Security, Inc.</td>
<td>Sarbari Gupta</td>
<td><a href="mailto:3pao@electrosoft-inc.com">3pao@electrosoft-inc.com</a></td>
</tr>
<tr>
<td>Electrosoft Services, Inc.</td>
<td>Rod Volz</td>
<td><a href="mailto:rhvolz@emesec.net">rhvolz@emesec.net</a></td>
</tr>
<tr>
<td>EmeSec Incorporated</td>
<td>Sean Cope</td>
<td><a href="mailto:sean.cope@homelandsecurityconsultants.net">sean.cope@homelandsecurityconsultants.net</a></td>
</tr>
<tr>
<td>Homeland Security Consultants</td>
<td>James Biggs</td>
<td><a href="mailto:james@jdbiggs.com">james@jdbiggs.com</a></td>
</tr>
<tr>
<td>J.D. Biggs and Associates, Inc.</td>
<td>Paul Nguyen</td>
<td><a href="mailto:paul.nguyen@knowledgecg.com">paul.nguyen@knowledgecg.com</a></td>
</tr>
<tr>
<td>Knowledge Consulting Group, Inc.</td>
<td>Robert Dumais</td>
<td><a href="mailto:rdumais@logyx.com">rdumais@logyx.com</a></td>
</tr>
<tr>
<td>Logyx LLC</td>
<td>Waylon Krush</td>
<td><a href="mailto:fedramp@lunarline.com">fedramp@lunarline.com</a></td>
</tr>
<tr>
<td>Lunarline, Inc.</td>
<td>Yong-Gon Chon</td>
<td><a href="mailto:yong-gon.chon@secureinfo.com">yong-gon.chon@secureinfo.com</a></td>
</tr>
<tr>
<td>Secure Info</td>
<td>William Bell</td>
<td><a href="mailto:william_bell@sra.com">william_bell@sra.com</a></td>
</tr>
<tr>
<td>SRA International, Inc.</td>
<td>Michael Carter</td>
<td><a href="mailto:fedramp@verisgroup.com">fedramp@verisgroup.com</a></td>
</tr>
</tbody>
</table>
Joint Authorization Board (JAB)

• The “panel of judges”
• performs risk authorizations and grants the provisional ATO
• members are the CIOs from the Department of Homeland Security (DHS), the General Services Administration (GSA), and the Department of Defense (DoD)
Provisional ATO

- This is the ATO the CSPs get from the JAB
- A customer agency can leverage this ATO for most/all controls but will still need another ATO from their local AO
- The agency AO may be satisfied with what is covered under the provisional ATO, or may require additional controls to be satisfied on that agency’s end
The Process – Very Much Like NIST RMF

- Same terms
- Same roles
- Based on same control catalog
- Same basic phases

FedRAMP Templates

Below, please find all FedRAMP templates listed individually for your perusal and use:

Template Files

- Contingency Plan Template
- Control Implementation Summary Template
- Control Tailoring Workbook (CTW) Template
- e-Authentication Template
- FIPS 199 Template
- Plan of Action and Milestones (POAM) Template
- Privacy Threshold Analysis and Privacy Impact Assessment (PTA & PIA) Template
- Rules of Behavior (RoB) Template
- Security Assessment Plan (SAP) Template
- Security Assessment Report (SAR) Template
- Security Assessment Test Cases
- Self-Attestation Template
- System Security Plan (SSP) Template
Control Set

- FedRAMP control set based on NIST SP 800-53 Rev 3
- Low and Moderate baselines only for FedRAMP systems
- Uses Low and Moderate baselines from 800-53 Rev 3 but adds additional “Not Selected” controls deemed relevant to cloud environments
- For controls with parameter requirements, those were defined by the JAB
Control Set

FedRAMP Low and Moderate baselines are more stringent than default NIST 800-53
System Security Plan (SSP)

• Just like NIST RMF, the FedRAMP SSP is one of the core documents for the authorization package

• It contains 80-90% of the same fields as the traditional NIST 800-18-based SSPs we’ve all seen

• Fields like: System name, info types, security category, POCs, system description, environment description, etc.
System Security Plan (SSP)

• Reminiscent of the early C&A days, the FedRAMP SSP weighs in at 352 pages! – the empty template!
Why is it so BIG?

• To be fair, all but ~30 pages are dedicated to implementation narratives
• There are a lot of new fields required to describe a cloud system
• They took a cue from DoD and added a PPSM section
New Fields and Sections in the SSP

8.1 CLOUD SERVICE MODEL

Information systems, particularly those based on cloud architecture models, are made up of different service layers. The layers of the <Information System Name> that are defined in this SSP, and are not leveraged by any other Provisional Authorizations, are indicated in the table that follows.

<table>
<thead>
<tr>
<th>Service Provider Architecture Layers</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Software as a Service (SaaS)</td>
<td>Major Application</td>
</tr>
<tr>
<td>Platform as a Service (PaaS)</td>
<td>Major Application</td>
</tr>
<tr>
<td>Infrastructure as a Service (IaaS)</td>
<td>General Support System</td>
</tr>
<tr>
<td>Other</td>
<td>Explain:</td>
</tr>
</tbody>
</table>
New Fields and Sections in the SSP

- One new section obviously influenced by DoDI 8551.1, Ports, Protocols, and Services Management (PPSM)
- Great DoD concept, not usually seen in a NIST RMF SSP

### 10.1.5 Ports, Protocols and Services
The table below lists the Ports, Protocols, and Services enabled in this information system. TCP ports are indicated with a T and UDP ports are indicated with a U.

<table>
<thead>
<tr>
<th>Ports (T or U)</th>
<th>Protocols</th>
<th>Services</th>
<th>Purpose</th>
<th>Used By</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
New Fields and Sections in the SSP

Every control in Section 13 has these new fields (x hundreds)

<table>
<thead>
<tr>
<th>Responsible Role:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter:</td>
</tr>
<tr>
<td>Implementation Status (check all that apply):</td>
</tr>
<tr>
<td>Implemented</td>
</tr>
<tr>
<td>Partially implemented</td>
</tr>
<tr>
<td>Planned</td>
</tr>
<tr>
<td>Alternative implementation</td>
</tr>
<tr>
<td>Not applicable</td>
</tr>
<tr>
<td>Control Origination (check all that apply):</td>
</tr>
<tr>
<td>Service Provider Corporate</td>
</tr>
<tr>
<td>Service Provider System Specific</td>
</tr>
<tr>
<td>Service Provider Hybrid (Corporate and System Specific)</td>
</tr>
</tbody>
</table>
Responsibility for Controls

From FedRAMP CONOPS
Continuous Monitoring / Ongoing A&A

Ongoing Assessment & Authorization

Ongoing assessment and authorization, often referred to as continuous monitoring, is the third and final process for cloud services in FedRAMP. Ongoing A&A ensures that the security controls implemented during the security authorization remain effective.

There are three key areas associated with Ongoing A&A detailed below:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operational Visibility</td>
<td>Operational visibility provides visibility into the security control implementations through (1) automated data feeds, (2) periodically submitted specific control evidentiary artifacts, and (3) annual self-attestation reports.</td>
</tr>
<tr>
<td>Change Control Process</td>
<td>Change control relates to (1) any changes or proposed changes that significantly impact the CSP’s ability to meet FedRAMP requirements as well as the oversight of a CSP's management it’s Plan of Action and Milestone’s (POA&amp;Ms).</td>
</tr>
<tr>
<td>Incident Response</td>
<td>Incident response focuses on new risks and vulnerabilities that affect authorized system and all response and mitigation activities needed to maintain the security of a system.</td>
</tr>
</tbody>
</table>
The Repository, aka “where you go shopping”

• When a CSP finally gets their Provisional ATO, their A&A documents go into “the Repository”

• Federal customers looking for a CSP can do their “shopping” here

• There is an NDA-like process, where the potential customers promise not to talk about sensitive data disclosed in the A&A documents

• In turn, the customers get access to the repository and look through the systems and compare and find the best fit for them
## The Repository

### Security Assessment Package Categories

<table>
<thead>
<tr>
<th>Category Name</th>
<th>Assessed by</th>
<th>Authorizing Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSP Supplied</td>
<td>Accredited 3PAO</td>
<td>N/A – no JAB, no Agency</td>
</tr>
<tr>
<td>CSP own, in-house, using own ISSOs</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Agency ATO*</td>
<td>Any 3PAO*</td>
<td>Agency</td>
</tr>
<tr>
<td>Agency chooses CSP not in Repos, Agency ISSOs, and 3PAO not accredited</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Agency ATO w FedRAMP 3PAO</td>
<td>Accredited 3PAO</td>
<td>Agency</td>
</tr>
<tr>
<td>Agency chooses CSP not in Repos, Agency ISSOs, and Accredited 3PAO</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FedRAMP Provisional Auth</td>
<td>Accredited 3PAO</td>
<td>JAB (+ Agency)</td>
</tr>
<tr>
<td>Agency chooses CSP not in Repos, Agency ISSOs, and Accredited 3PAO</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

All examples listed follow FedRAMP and report to PMO

*Not eligible for JAB review and Provisional Authorization*
We Talked About FedRAMP...
What About Archer?
RSA Archer, A&A, and CM

- We have two versions of A&A and CM offerings on the roadmap for 2013
- We have a functional demo of the NIST RMF environment you can see now – email me and I will point you in the right direction

chris.hoover@rsa.com
One great feature about our A&A environment is the ability to accommodate many control sets...

Including the FedRAMP control catalog!
Applications: 3PAO

- If you are a 3PAO, the RSA Archer A&A tool can be used to perform system definition/phase 1/SSP
- It can also be used to perform and track the assessments for the Provisional ATO
Applications: Federal Customer

If you are a federal customer, and you have responsibility for a portion of FedRAMP controls not covered by the CSP...

...Archer can manage your normal A&A workload using traditional 800-53 control set and manage your FedRAMP requirements using that control set.
Questions?

chris.hoover@rsa.com
Upcoming RSA Events

• RSA Conference 2013 – San Francisco, Feb. 25 – March 1 @ Moscone Center
  Register Now:  https://community.emc.com/events/1745

• RSA Archer GRC Summit 2013 – Washington, D.C., June 12-14 (Registration Info Coming Soon)
Free Friday Tech Huddle

- Join the ‘customer only’ weekly Free Friday Tech Huddle live webcasts @ 12 ET
- Customer Support team addresses how to troubleshoot common issues & utilize new functionality delivered by the RSA Archer products
- Join us!

https://community.emc.com/docs/DOC-18975
RSA Archer Public Webcast – every Thursday

• Feb 7 at 2ET:  PCI Compliance
• Feb 14 at 10ET:  Solvency II and GRC

Register on the RSA public website
http://www.emc.com/campaign/global/rsa/rsa-webcast.htm
THANK YOU

chris.hoover@rsa.com