

# Mutual Monitoring Update

Final Report

A.J. Stein

OMS Cybersecurity Masters Practicum

Georgia Institute of Technology

PUBP-6727 OCY

# The Problem

- Cloud computing infrastructure is essentially ubiquitous.
- Cloud service providers must cater to customers, especially regulated ones.
- A major barrier is ongoing evaluation of the provider's cybersecurity posture.
- The results are often centralized bureaucracies.

## The Problem

- Are cloud security bureaucracies the right way?
- Are they the only way?
- Who watches the watchers?



FedRAMP

# The Solution

- Analyze FedRAMP ConMon's strengths and weaknesses.
- Design an alternative model.
  - Stakeholders mutually monitor each other with transparency services.
  - Forgo control-driven assessment, focus measurable security properties.
  - Use a simple quantitative framework for measuring properties.
- Do not certify, do not authorize, but **measure** *each other*.

# Background

- What is FedRAMP?
- What is FedRAMP ConMon?
- What works? What doesn't?

## What is FedRAMP?

In mid-2009, an interagency effort, created under the Federal Cloud Computing Initiative, was established to focus on solving a single problem statement—How do we best perform security authorization and *continuous monitoring for out-sourced and multiagency systems*?

Metheny, M. (2017). Introduction to the federal cloud computing strategy. In Federal Cloud Computing (pp. 239). Elsevier. <https://doi.org/10.1016/b978-0-12-809710-6.00001-9>

## How Did FedRAMP Evolve?

2011 December: FedRAMP policy signed

2012 May: Announcement of third party auditors

2012 June: FedRAMP officially launches

2012 December: First provisional FedRAMP authorization

2013 May: First full authorization of AWS with HHS

<https://www.nextgov.com/modernization/2016/05/a-brief-history-of-fedramp/218162/>

## How Did FedRAMP Evolve?

2014 June: Deadline for agency compliance from policy

2014 December: Announcement of FedRAMP Forward

2016 March: Revised JAB process and prioritization timelines

2022 December: FedRAMP Act codified into law

2023 October: Draft modernization memo published

<https://www.nextgov.com/modernization/2016/05/a-brief-history-of-fedramp/218162/>



## How Did FedRAMP Evolve?

2024 March: Centralized platform announced

2024 July: M-24-15 disbands JAB; established new FedRAMP board

2024 July: M-24-15 requires agency uploads to platform by July 2025

2025 March: Centralized platform contract halted

2025 April: FedRAMP downsizes most contractor staff

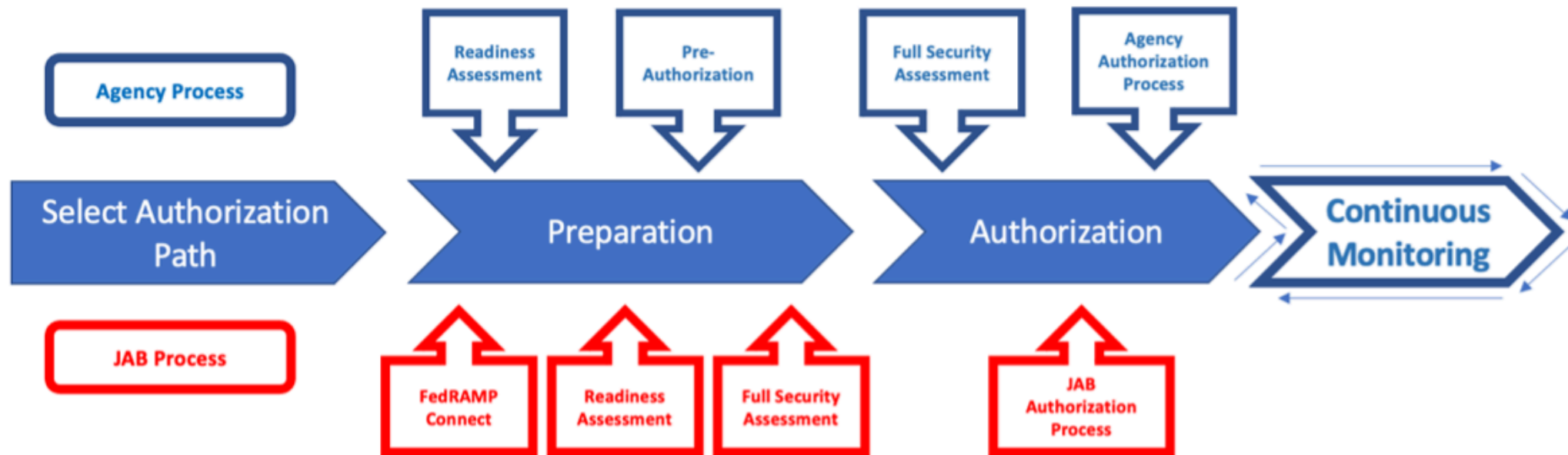
2025 March: 20x Modernization Pilots and KSIs announced

2025 May: Announcement of secure storage standard

<https://www.fedramp.gov/updates/changelog/>

# What Were the FedRAMP Processes? (+ JAB)

## FedRAMP Authorization Process



**Note:** Readiness Assessment is required for the JAB Process and is optional but highly recommended for the Agency Process

# What Are the FedRAMP Processes? (— JAB)

## 01 Preparation

### Readiness Assessment

(Optional, but highly recommended)

- RAR Development
  - FedRAMP PMO Review of RAR
  - Remediation (if needed)
- FedRAMP Marketplace Designation – Ready



### Pre-Authorization

- Partnership Establishment
- Authorization Planning
- Kickoff Meeting
- FedRAMP Marketplace Designation – In Process

## 02 Authorization

### Full Security Assessment

- Security Authorization Package (SSP, SAP, SAR, POA&M)\*



### Agency Authorization Process

- Agency Review of Security Authorization Package
- SAR Debrief
- Remediation
- Agency Final Review
- Agency Issues ATO
- FedRAMP PMO Review
- Remediation (if needed)
- FedRAMP Marketplace Designation - Authorized

## 03 Continuous Monitoring

### Post Authorization

- Ongoing Continuous Monitoring Deliverables
- Annual Assessment

\* The full security assessment may be prepared in advance of the authorization phase, or completed during the authorization phase. This is dependent on the agency's review approach.

## What is FedRAMP ConMon?

- Monthly assessments
  - Updated inventory scans
  - Updated vulnerability scans
- Significant change requests
- Annual assessments

**What works?**

**What doesn't?**

**Solution**

**Prototyping**

**Architecture Specification**

# **Solution Evaluation**



## **Solution Limitations**

## **Next Steps and Future Work**

# Feedback

- You can provide feedback in multiple ways.
- Post in the class discussion board in Canvas.
- Open issues in my GitHub repo at [github.com/aj-stein/practicum/issues](https://github.com/aj-stein/practicum/issues).



# Conclusion

Et fin.

(Find me on the Internet if you want to learn more.)