# Federal Risk and Authorization Management Program (FedRAMP)

## Getting started on the FedRAMP Security Authorization Process for Cloud Service Providers

November 7, 2012

GSA

FedRAMP SM

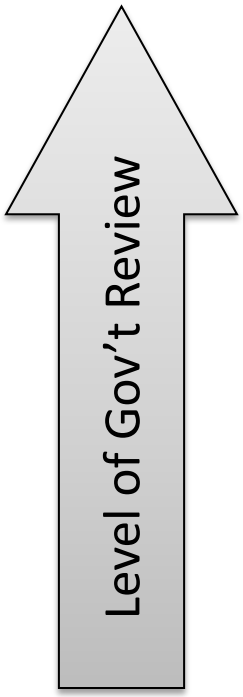
# Today's Webinar

*FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud services.*

- This webinar describes what is required to complete the initial step in the FedRAMP process and covers topics from "before you begin" through defining the security authorization boundary and delineating between consumer and provider responsibilities.

# Access Points for FedRAMP Secure Repository

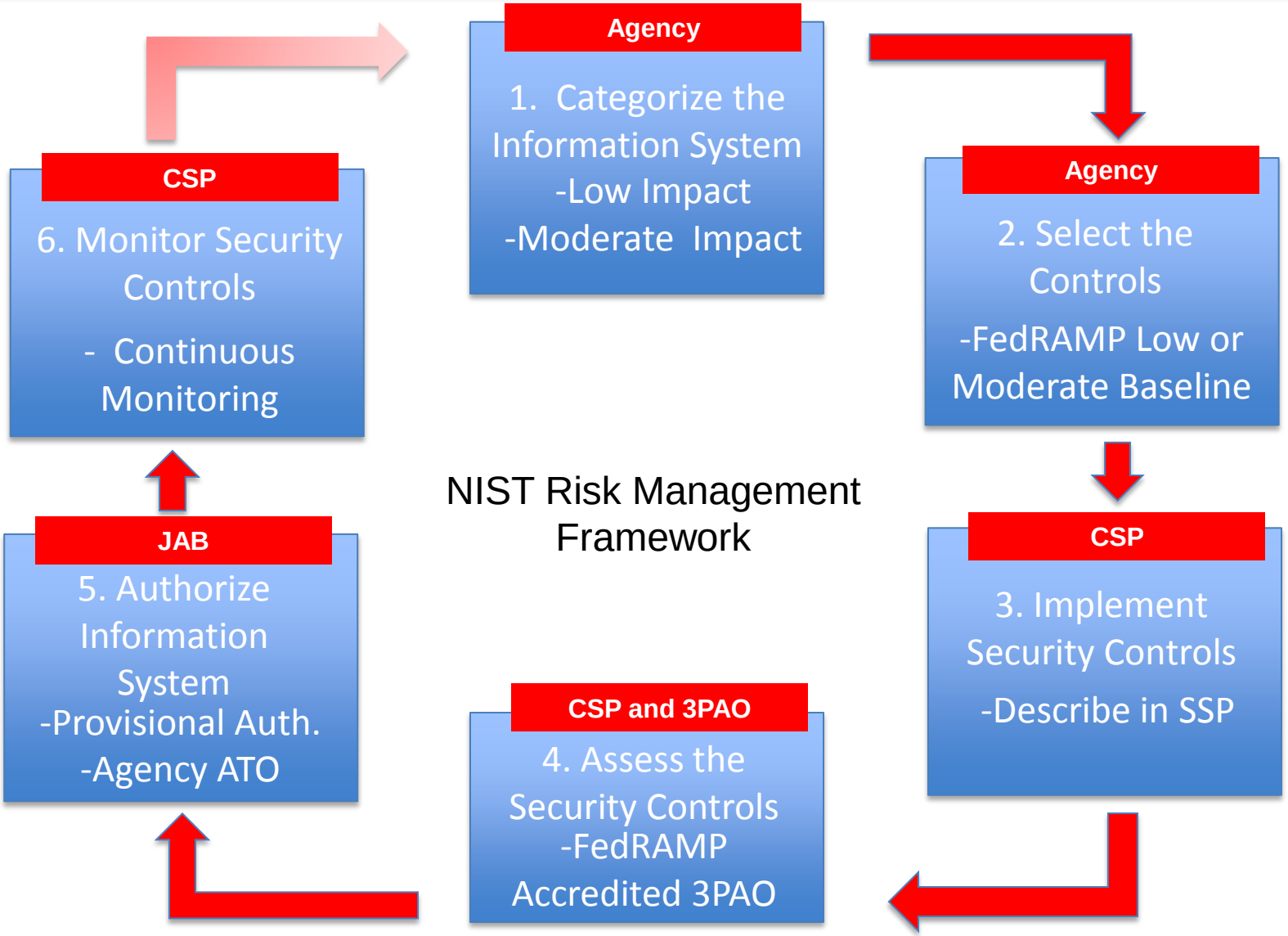
| Authorization Level | FedRAMP 3PAO | ATO Status |
|---|---|---|
| JAB Provisional Authorization | ✓ | JAB (+Agency) |
| Agency ATO with FedRAMP 3PAO | ✓ | Agency |
| Agency ATO** | ✗ | Agency |
| CSP Supplied | ✓ | n/a |




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

*3PAO – Third Party Assessment Organization*

# How Does FedRAMP Relate to the NIST Process?

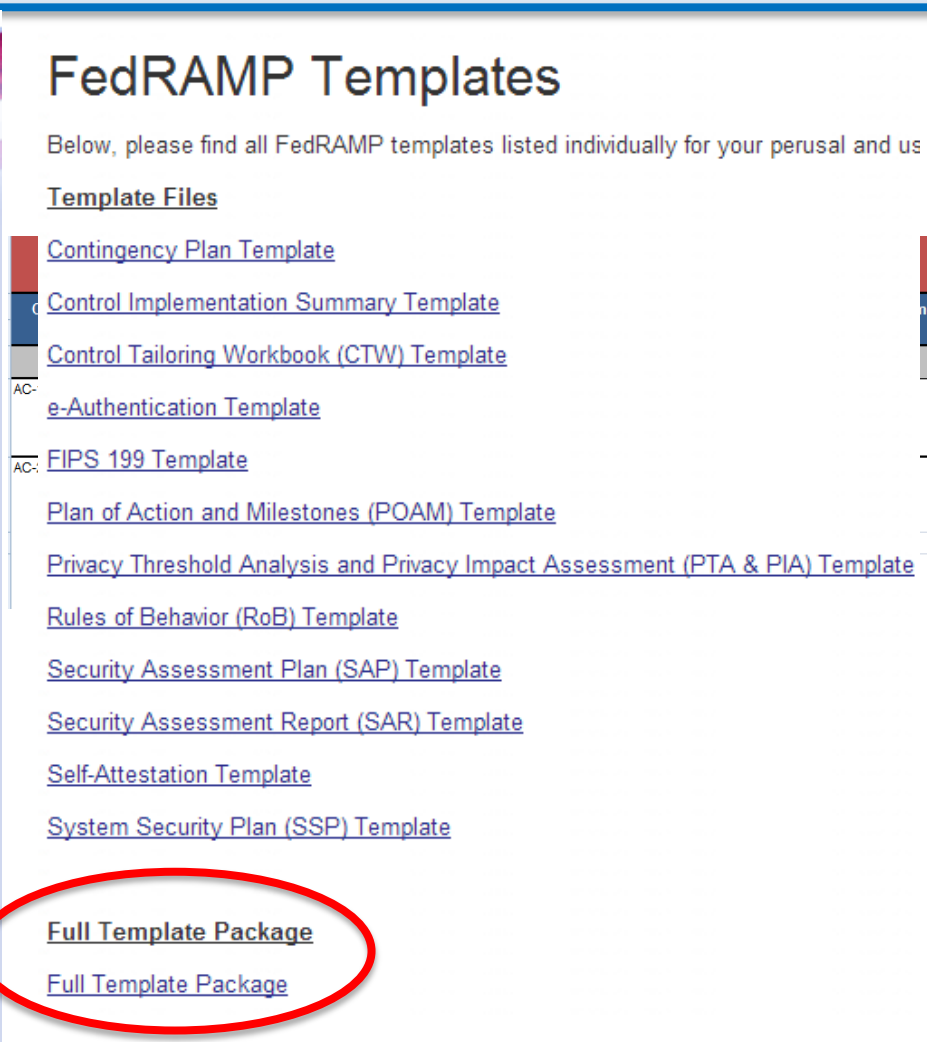


# Before You Get Started - FedRAMP.gov a Resource Treasure Trove



# FedRAMP.gov a Resource Treasure Trove (cont'd)





# How to Apply


The Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

Are you a...?

| Federal Agency | CSP *Cloud Service Provider* | 3PAO *Third Party Assessors* |
|---|---|---|
| *What can FedRAMP do for your agency?* | *Get a FedRAMP security authorization.* | *Become a FedRAMP accredited assessor.* |

FEDRAMP HAS NOW LAUNCHED

To apply or sponsor a system for authorization, please fill out the FedRAMP application here.

**CONTACTS**

**General Inquiries**
info@fedramp.gov

**Press Inquiries**
202-501-9113

**KEY LINKS**

FedRAMP Initiation Request

Accredited 3PAOs

Authorized CSPs

**KEY DOCUMENTS**

FedRAMP Concept of Operations (CONOPS)

FedRAMP Security Controls

FedRAMP Templates

FedRAMP Continuous Monitoring Strategy Guide

FedRAMP Standard Contract Clauses

FedRAMP Control-Specific Contract Clauses

Guide to Understanding FedRAMP

FedRAMP Policy Memo (OMB)

3PAO Program Description

FedRAMP JAB Charter

## FedRAMP Initiation Request

Please complete the form below by providing the requested information

Requesting Organization Information

* Organization Name:

* Street Address: * City:

* State: Please enter two character state code in uppercase, if outside of US, please enter NA * Postal Code: * Country:

Requesting Organization Points of Contact

Primary Point of Contact:

* First Name: * Last Name:

* Title:

* Phone: Please enter phone in (XXX) XXX-XXXX format * Email:

Secondary Point of Contact:

* First Name: * Last Name:

* Title:

* Phone: Please enter phone in (XXX) XXX-XXXX format * Email:

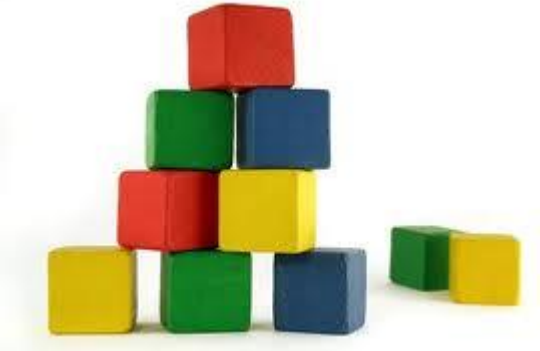
Back-up Point of Contact:

First Name: Last Name:

Title:

Phone: Please enter phone in (XXX) XXX-XXXX format Email:

# Time to Begin Your Documentation



Foundation…

Resources…

You've applied…

Time to start documentation.

# After You Apply

- Expect a preliminary call from the FedRAMP PMO
  - Establish communications
  - Confirm application information
  - Answer questions concerning FedRAMP

- Determine the best and quickest path to get into the FedRAMP Repository
  - Review existing documentation
  - Understand current relationships and ATO status with existing customer agencies
  - Identify overall readiness to pursue JAB provisional authorization

# Keys to Proper Documentation Development

Key Areas of Focus for Documentation

- Completeness
- Compliant with FedRAMP policy and consistency with other package documents
- Delivery of supporting documentation
- Documentation is adequately referenced – e.g. : Policy, SOPs, Rules of Behavior, common control catalogs, waivers, exceptions, etc.

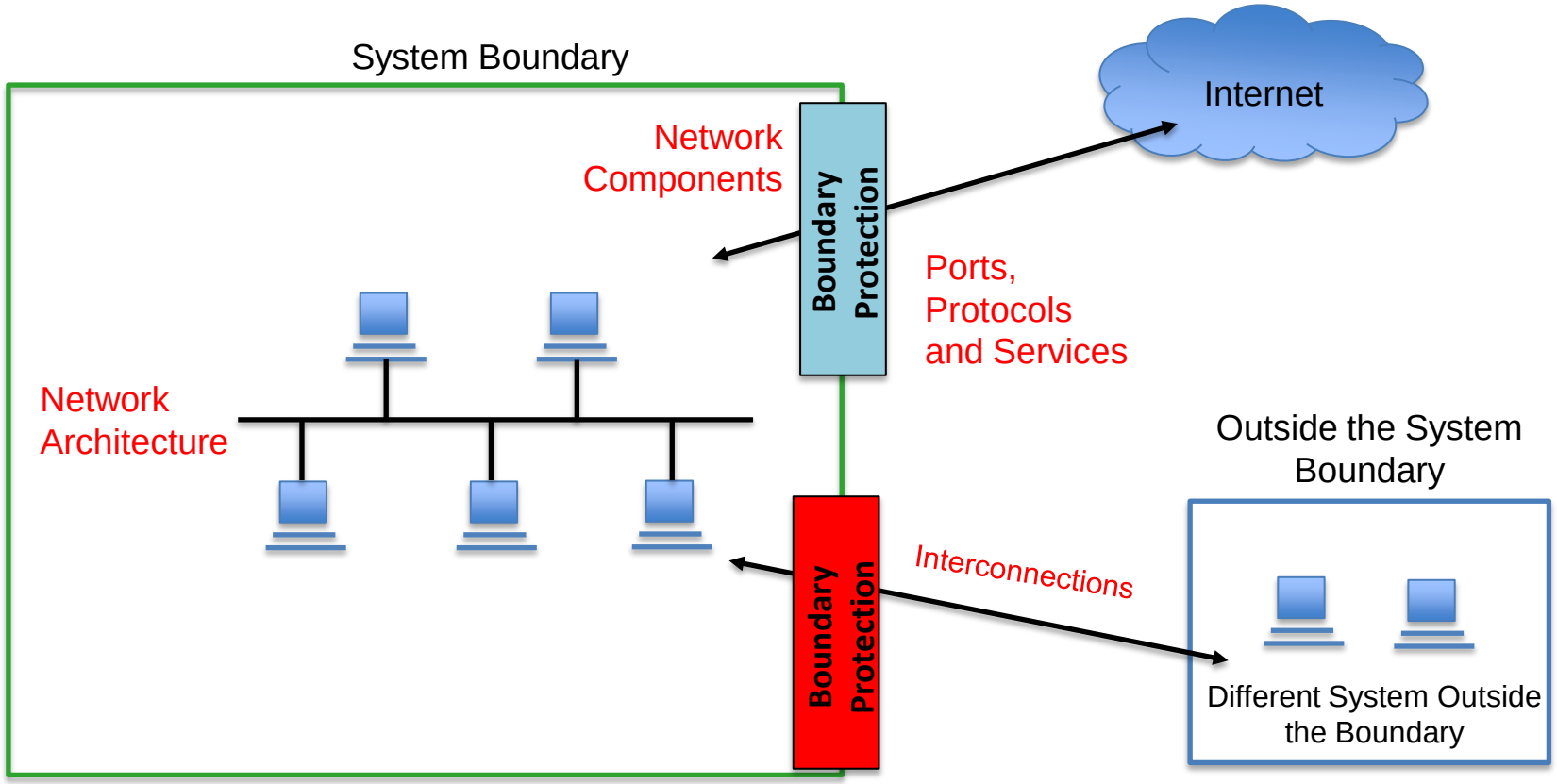
Content should address four (4) criteria :

1. **What**
2. **Who**
3. **When**
4. **How**

Proper level of detail for responses should be:

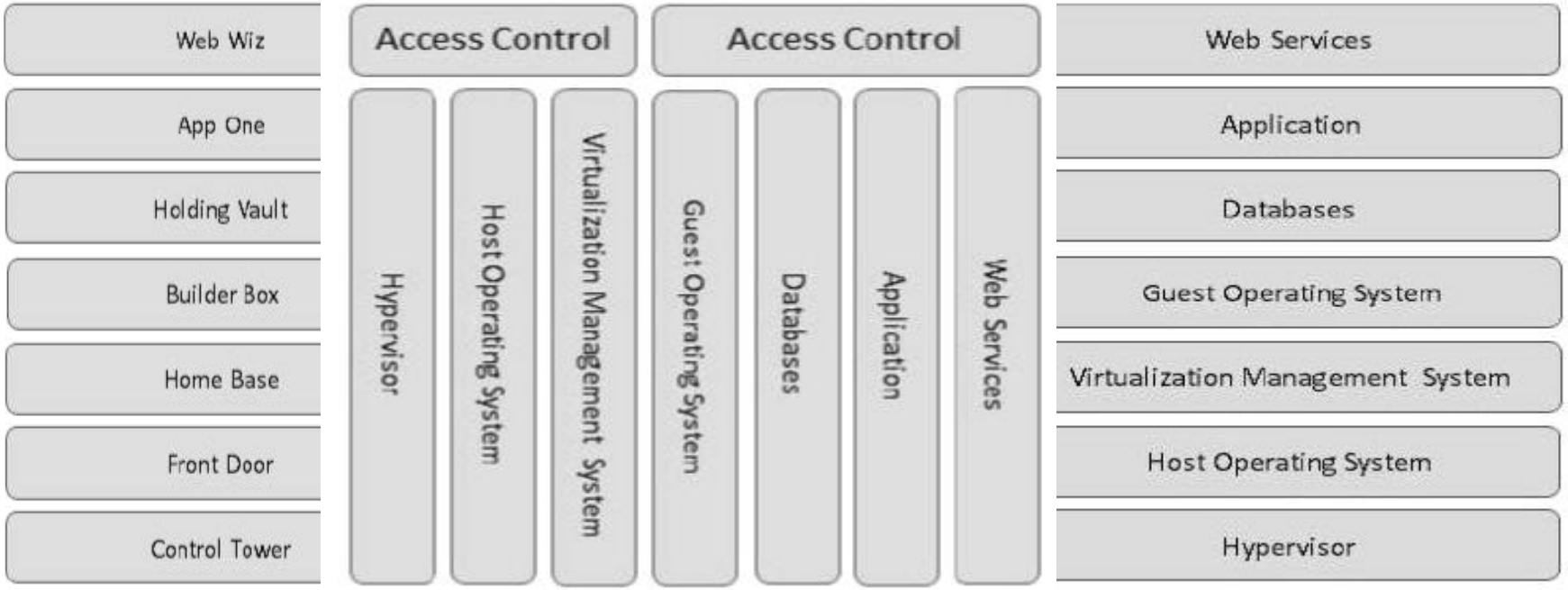
- Unambiguous
- Specific
- Complete
- Comprehensive
- Make sure the response is sufficient in length to properly answer the question

# Describing Boundaries in the System Security Plan (SSP)




- Understand which IT assets fit within the boundary.
- Interconnections - Indicate and label interconnections to other systems
- Indicate the hardware and software
- Make sure your diagrams are consistent with boundary descriptions

# Describing Components in the SSP




Components by Name

Components Grouped by Controls

Components by Function

- Keep naming convention consistent
- Group components by controls
- If multiple controls are used describe which controls affect each component

# Describing Security Controls in the SSP

- Security Control and enhancement requirement.
- Security control and enhancements require security control summary information.
- NOTE: The "-1" controls (e.g. AC-1, SC-1 etc.) describe Policies and Procedures.

**Control Summary Definition**

Responsible Role: In the field described as Responsible Role, the CSP should indicate what staff role within their organization is responsible for maintaining and implementing that particular security control. Examples of the types of role names may differ from CSP to CSP but could include role names such as:

•System Administrator
•Database Administrator
•Network Operations Analyst
•Network Engineer
•Configuration Management Team Lead
•IT Director
•Firewall Engineer

### 13.7.2 User Identification and Authentication (IA-2)

The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).

| IA-2 | Control Summary Information |
|---|---|
| Responsible Role: | |
| Parameter: | |
| Implementation Status (check all that apply):<br>☐ Implemented<br>☐ Partially implemented<br>☐ Planned<br>☐ Alternative implementation<br>☐ Not applicable | |
| Control Origination (check all that apply):<br>☐ Service Provider Corporate<br>☐ Service Provider System Specific<br>☐ Service Provider Hybrid (Corporate and System Specific)<br>☐ Configured by Customer (Customer System Specific)<br>☐ Provided by Customer (Customer System Specific)<br>☐ Shared (Service Provider and Customer Responsibility)<br>☐ Inherited from pre-existing Provisional Authorization (PA) for <Information System Name>, <Date of PA> | |

| IA-2 What is the solution and how is it implemented? |
|---|
| |

# System Security Plan Reality Check

- SSP template is 352 pages long
- Long template required to assure the system and implementation of controls are properly documented
- Effort to produce a well documented SSP leads to a smooth process
- SSP Quick Tips
  - Is your hardware and software inventory complete?
  - Are components from the inventory represented on your network map?
  - Have you provided a response for all sections of the control and the control enhancement?

# In Summary…

- A little prep will ensure a smooth assessment process
- Review the FedRAMP Baseline Controls and SSP Template
- Read the Guide to Understanding FedRAMP
- Review the Prep Checklist
- Apply to FedRAMP

# Question and Answer Session

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

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

Follow us on twitter @ FederalCloud

GSA


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

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

Follow us on twitter @ FederalCloud