

Dec. 2010 - Dec. 2011

**DEC. 2014 - JUN. 2015**  
Progress over 6 months

Jun. 2015 - Dec. 2015

Dec. 2015 - Jun. 2016

Jun. 2016 - Dec. 2016



# FedRAMP FORWARD

A LOOK BACK AT THE LAST 6 MONTHS

## FedRAMP EXISTS TO:



Protect taxpayer information



Save money



Modernize government

## Challenge.gov COMPETITION

CREATE A TOOL TO AUTOMATE CSP REVIEW

**PRIZE \$250,000**



## BASELINE FedRAMP USE ACROSS GOVERNMENT

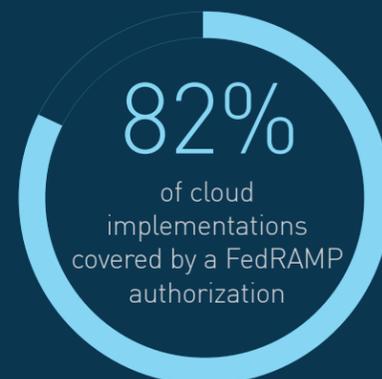
Increase of authorized CSPs in the last 6 months



- 18 JAB
- 17 Agency
- 3 CSP supplied

Cloud implementations in government

**> 1400**



## PARTNERSHIPS with Industry and Agencies

FedRAMP identified opportunities to partner:

- With **DHS**: to develop a TIC overlay
- With **Industry**: to map FedRAMP controls to CSA CCM (via the Cloud Security Alliance)
- With **Agencies**: to pilot FedRAMP high-impact systems and standardize continuous monitoring



## FEEDBACK



Solicited and acted on feedback:

- Received and acted on over **1000 comments** in regard to High Baseline
- Received and acted on over **300 comments** in relation to TIC overlay
- Requesting comments on 3PAO requirements through August 20

## DO ONCE, USE MANY TIMES

**\$70 MILLION**

per year in cost avoidance as a result of FedRAMP authorization re-use

## TRAINING

Launched a free online training program

IN 5 MONTHS



OVER **500** ENROLLEES

## TRENDS IN FEDERAL CYBERSECURITY

- SPENDING
- THREAT

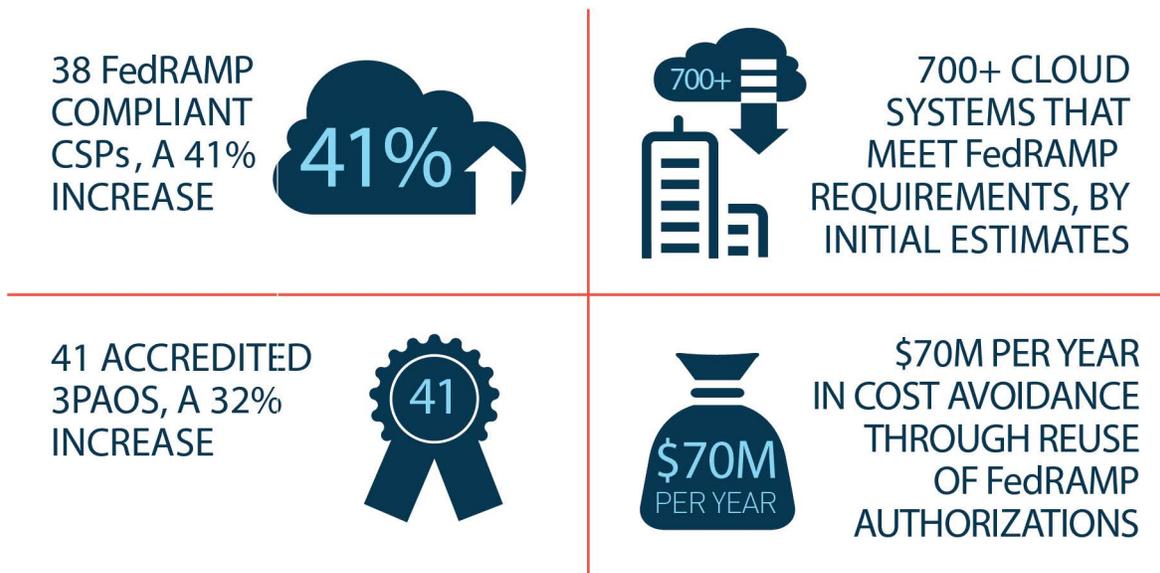


Since its peak in 2010, Federal IT investment continues to decrease, while government data boundaries and cyber threats increase.



It's been six months since we released "FedRAMP Forward: Two Year Priorities." During that time, we worked on 14 initiatives to help make progress in each of our three focus areas: engaging stakeholders, increasing efficiencies, and continuing to adapt. It's time to see what we've accomplished and give some updates to our overall goals moving forward.

First, though, we need to see where we are compared to six months ago. As of the end of June:



It has been an exciting past six months with lots of progress. The sections below go into each initiative in greater detail.

### BASELINE FedRAMP USE ACROSS THE USG

To develop an initial baseline of cloud usage across the federal government, we analyzed agency PortfolioStat reporting data and CSP customer surveys. The initial baseline shows over 1,400 cloud instances representing over 80 cloud services in use across the US Government. Of those, 82% are FedRAMP compliant. Ultimately, we know there is a significant gap between reported use by vendors and agencies and actual use. If anyone knows of a perfect aggregate data source, let us know! Until that source exists, we will continue to normalize this baseline on a quarterly basis by adding additional authoritative data sources and additional CSP responses.

The initial baseline shows over 1,400 cloud instances representing over 80 cloud services in use across the US Government. Of those, 82% are FedRAMP compliant.

### PROVIDE PRACTICAL IMPLEMENTATION GUIDANCE FOR AGENCIES USING FedRAMP

Reuse of FedRAMP authorizations significantly reduces the burden on an agency to secure its cloud instances. We published the *Agency Guide for FedRAMP Authorizations* detailing how agencies can reap significant savings through reusing existing authorizations. This reuse will eliminate the time required to document and assess the CSP environment, which could eliminate 50-90% of the authorization work required. Put into other words, this guide helps agencies understand how to functionally reuse existing FedRAMP authorizations to bring secure cloud services online without having to slash and burn other areas of their operation or budget.



## PUBLISH MULTI-AGENCY METHODOLOGY FOR FedRAMP COLLABORATION

We developed the FedRAMP Guide for Managing Multi-Agency Continuous Monitoring to let agencies know how they can work together to jointly, continuously monitor cloud systems they use. Collaborating in this way gets to the heart of our “do once, use many times” framework. By getting agencies to speak from a collective customer voice and allowing CSPs to work with all of their customers in one setting, we’re building an environment of collaboration and risk mitigation. Over the next six months we’ll pilot this collaboration with agencies and continue to expand the guide to include initiating an authorization of a CSP by multiple agencies.

## LAUNCH ONLINE FedRAMP TRAINING

Being an informed stakeholder doesn’t happen through osmosis. To better educate members of our community, we launched a free online training program on [www.FedRAMP.gov](http://www.FedRAMP.gov). Our first two courses, “Introduction to FedRAMP” and “FedRAMP SSP Required Documents,” had over 500 people register within the first five months. We’re happy to see the number of informed, FedRAMP enthusiasts is ever increasing. We’ll continue to roll out new trainings to keep it up!

Since our relaunch in March, over 95,000 users have visited our site with traffic increasing by more than 10,000 users month over month.

## RE-LAUNCH FedRAMP.GOV

FedRAMP.gov is our official communication vehicle to all of our stakeholders. We recognized the old site’s clunky interface and text heavy pages did not effectively serve FedRAMP’s mission. We relaunched our website to enhance user interface, simplify access to important information, and provide new capabilities (like our handy training program). Since our relaunch in March, over 95,000 users have visited our site, with traffic increasing by more than 10,000 users month over month.

## PUBLISH AGENCY PROCUREMENT GUIDANCE WITH OMB

Agencies and CSPs have expressed the need for clearer guidance on how to incorporate FedRAMP into acquisitions. Given that agencies are required to enforce FedRAMP compliance through their contracts with CSPs, increased contract compliance is a big part of that. We worked closely with OMB e-Gov and OFPP to develop guidance for contracting officers to meet these requirements. A draft of this guidance will go through additional reviews by OMB, agencies, and targeted acquisition communities beginning in August with an expected publication date of October 31, 2015.

## PUBLISH GUIDELINES TO ADDRESS 3PAO INCONSISTENCIES

Since launching the 3PAO accreditation program, we have accredited 41 3PAOs. As a cornerstone of the assessment process and one of our key stakeholder groups, we recognized the need to provide enhanced guidance and direction to our 3PAOs, while at the same time to increase oversight and ensure consistency of the work products our 3PAOs produce. To that end, we developed two guidance documents to help 3PAOs better baseline their work. The first document, *The FedRAMP JAB P-ATO Vulnerability Scan Requirements Guide*, explains the level of detail and information required for scanning of CSP systems. Document number two, *FedRAMP Penetration Testing Guidance*, provides guidance on what must be included during a 3PAO’s penetration testing of a CSP system. Additionally, we published a draft update to 3PAO certification requirements, which is currently out for public comment. This is the first update to the 3PAO requirements and will be finalized within the next six months.

## IDENTIFY AUTOMATION CAPABILITIES

We have seen an exponential growth in demand for JAB authorizations, which is exciting! However, we need to develop new ways to keep up. To better meet demand we’re partnering with Challenge.gov to release a competition to build an open-source, innovative solution to automate our quality reviews, with total prize money of \$250,000 (split between up to three winners). These reviews take an average of 24-



40 hours and usually require 3–4 FTEs to complete. We believe 75–90% of this process can be fully automated. These tools will be out and available to all stakeholders within 12 months.

### PUBLISH DRAFT REQUIREMENTS FOR REUSE OF EXTERNAL INDUSTRY COMPLIANCE

Over the course of the last six months, we worked closely with the Cloud Security Alliance (CSA) as they completed a mapping of the FedRAMP security controls to the CSA Cloud Controls Matrix (CCM). Based on this work, we've realized the mapping of FedRAMP/FISMA to other compliance frameworks is more complex than originally envisioned and would require more resources than we can dedicate. However, we've heard you loud and clear, this needs to be done! Over the next six months we'll be developing a call to action for industry to lead this effort in order to ensure that we continue to make progress on this.

### EVOLVE CONTINUOUS MONITORING

In late 2014, we solicited public feedback to identify ways we could evolve our continuous monitoring approach. Over the last six months we analyzed the responses in addition to conducting several interviews with key agency players. As a result, we are launching a pilot to take on the reporting responsibility for up to five agency authorizations for Continuous Monitoring. This would provide the same types of Continuous Monitoring reports for agency authorizations that we create for JAB authorizations. Over the next six months, this pilot will determine the scalability and feasibility of providing this service for all FedRAMP authorizations used by multiple agencies, regardless of who the initial authorizing official was.

We are launching a pilot to take on the reporting responsibility for up to five agency authorizations for Continuous Monitoring.

### PUBLISH GUIDELINES FOR AGENCIES TO MAINTAIN FedRAMP ATOs

Continuous monitoring provides the framework for agencies to ensure a CSP maintains an acceptable risk posture. We've developed the *P-ATO Maintenance and Revocation Guide* that details key indicators for determining risk and how to address these indicators with our CSPs. This guide is something we believe agencies should use as a model for their own processes when maintaining authorizations.

### PUBLISH DRAFT HIGH BASELINE REQUIREMENTS

In January we released a draft for public comment of the FedRAMP High Baseline requirements, developed through collaboration with DOD, DHS, HHS, VA, and DOJ (which represent 75% of all high systems across the USG). People had a lot to say. We received over 1,000 comments. Over the next six months, we will address all of the comments through cross-government tiger teams, re-release the draft for a second round of public comment, and finalize the baseline by the end of the calendar year. Additionally, we've identified four vendors to pilot completing a high authorization through the FedRAMP JAB while finalizing the baseline.

### DEVELOP A FedRAMP ASSESSMENT OVERLAY FRAMEWORK AND PUBLISH A DRAFT OVERLAY

We've worked closely with DHS's Trusted Internet Connection (TIC) Initiative over the past 18 months to develop an overlay demonstrating how CSPs meet the FedRAMP requirements and concurrently are able to provide Agencies TIC capabilities. We published the TIC overlay for public comment in April and received over 300 comments. We're currently working with the TIC office to address those comments and three vendors are piloting these capabilities through the CIO Council. Over the next six months we are targeting addressing two to three additional overlays with other program offices across the US Government like IPv6, HSPD-12 and the privacy community.