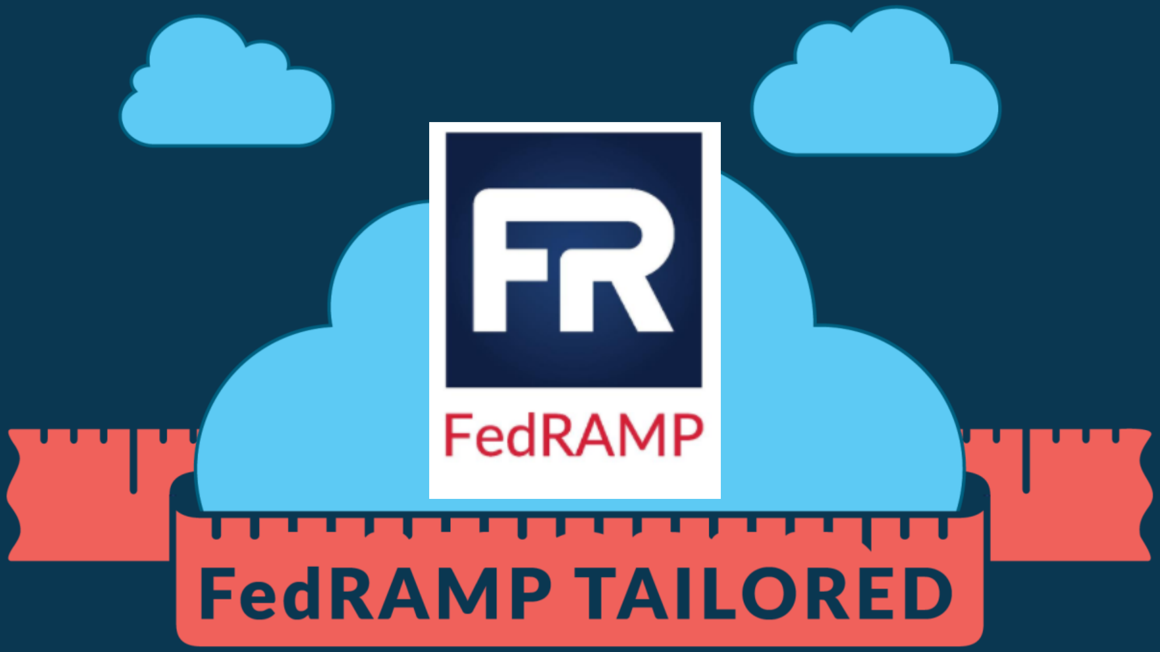


AN INTRODUCTION TO THE NEW SECURITY BASELINE

Ashley Mahan, *FedRAMP Evangelist*

June 2017 | www.fedramp.gov

FedRAMP Tailored: An Introduction

AGENDA

- Purpose and Outcomes
- Background
- Overview and Criteria
- Benefits
- Impact
- Next Steps
- Questions and Feedback

PURPOSE & OUTCOMES

Purpose and Outcomes

Purpose:

- To share FedRAMP's new security baseline for some low impact SaaS products.

Outcomes:

- A shared understanding of the intent of FedRAMP Tailored.
- Clarity on the situations when FedRAMP Tailored applies.
- A context within which to provide feedback and comments.

BACKGROUND

BACKGROUND

What Drove the Development

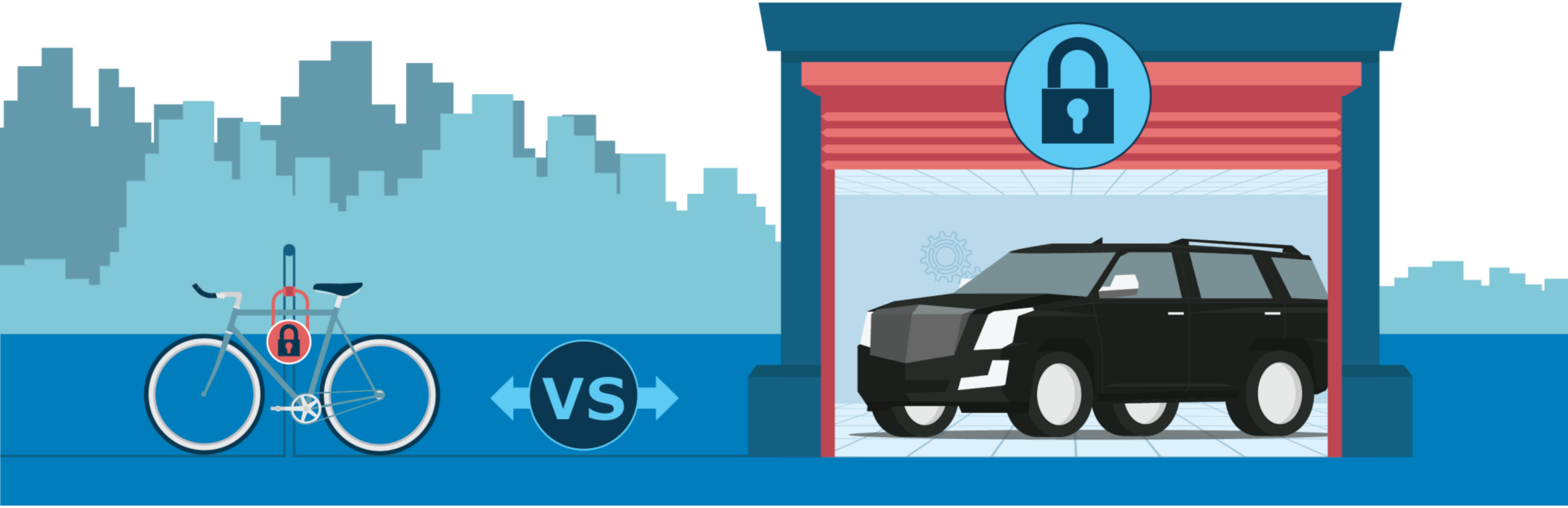
- Recent discussions with government digital service teams, CTOs, and CIOS revealed a business and mission need to use and authorize low-risk applications. It became clear that a traditional, one-size-fits-all security baseline has not worked well in achieving this goal.
- As a result of this, a portion of the CSP market was also being underserved and was unable to securely provide their service to the federal government.
- As FedRAMP expands further into SaaS, the one-size-fits-all approach can be adapted to fit specific use cases regarding different types of SaaS.
- FedRAMP Tailored was developed to meet this growing need and is designed to match the evolving needs of the government.
- Following NIST and OMB guidelines, FedRAMP Tailored is a useful way to provide government Authorizing Officials (AOs) with an approved standardized approach for determining the associated risks inherent in specific, unique low-impact cloud applications.

OVERVIEW & CRITERIA

OVERVIEW AND CRITERIA

Not all SaaS are Created Equal

- FedRAMP was originally built around enterprise-wide solutions that would cover the **broadest range of data types** for cloud architectures and low, moderate, and high impact
- **FedRAMP tailored addresses low risk use SaaS** —focusing on things like collaboration, project management, and open-source code development
- You would not secure your 2017 Cadillac Escalade the same way you would secure your Huffy Bike. You need a more rigorous security mechanism for the SUV, while a U-lock device will suffice to secure your bicycle.



OVERVIEW AND CRITERIA

Step 1: Categorize the Cloud Information System – FedRAMP Tailored categorizes low-impact SaaS solutions based on the following criteria:

1. Does the service operate in the cloud?
2. Is the cloud service fully operational?
3. Is the cloud service a SaaS, rather than an Infrastructure or a Platform?
4. Does the cloud service provide services without requiring the collection of personally identifiable information (PII)?
5. Is the cloud service low-security-impact, according to the FIPS 199 definition?
6. Is the cloud service hosted within a FedRAMP authorized infrastructure?

OVERVIEW AND CRITERIA

Step 2: Select Security Controls – FedRAMP Tailored allows agencies to select a smaller set of controls, based on information types and use.

Control Tailoring Action	Definition
Required, Required (Conditional)	Controls FedRAMP determined are required for Low Impact Cloud SaaS // Controls FedRAMP determined are conditionally required for Low Impact Cloud SaaS
Federal Responsibility	Controls that are uniquely Federal, which are primarily the responsibility of the Federal Government
Inherited	Controls FedRAMP determined to be inherited from the underlying infrastructure provider (i.e., FedRAMP authorized IaaS/PaaS) for Low Impact Cloud SaaS
Attestation	Controls for which FedRAMP determined that the CSP is required to attest to being in place for Low Impact Cloud SaaS
Not Related Specifically to Cloud Security (NSO)	Controls FedRAMP determined do not impact the security of Low Impact Cloud SaaS

OVERVIEW AND CRITERIA

Summary of FedRAMP Tailored Baseline:

Control Tailoring Action	Testing Required?	Attestation Required?	Number of Controls
Required, Required (Conditional)	✓	✗	36
Federal Responsibility	✗	✗	3
Inherited	✗	✗	8
Attestation	✗	✓	64
Not Related Specifically to Cloud Security	✗	✗	15
Total			**126**

✓ YES ✗ NO

OVERVIEW AND CRITERIA

Step 3: Implement Security Controls

CSPs must implement the controls and describe (in the FedRAMP *Tailored* templates) how the controls are employed within the information system and its environment of operation. CSPs must also clearly delineate control implementations that are the responsibility of the agency customer to implement in order to fully meet the intent of the security requirement.

Step 4: Assess Security Controls

Assessment of the implemented controls may be performed by an independent trusted third-party, such as a FedRAMP Accredited Third-Party Assessment Organization (3PAO), or the agency may perform the assessment. The degree of independence required is at the discretion of the Agency Authorizing Official (AO).

Step 5: Authorize System

An Agency AO must examine the implementation of the system and the risks associated with it in order to make a risk-based determination of its security posture. This is the basis for the Agency AO to authorize the system for use in their agency.

Step 6: Monitor Security Controls

Agencies must monitor the effectiveness of security controls for all authorized systems. CSPs must employ a program of continuous monitoring that includes assessing control effectiveness, documenting changes to the system or its environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system. CSPs must report on this program to Agency AOs for continued security authorizations for use.

BENEFITS

BENEFITS

Expected Benefits of FedRAMP Tailored:

- **Balance:** New baseline will provide agencies with agility to leverage valuable services while maintaining the appropriate level of security.
- **Simplicity:** The SSP, SAP, SAR, and Remediation Plans are combined into a single document (defined control-by-control). Separate attachments for the risk summary table and Plan of Action & Milestones (POA&M) are used for initial ATO and ConMon.
- **Speed:** This process can be completed in as little as 4 weeks.
- **Economical:** The simplified ATO documentation means Agencies and SaaS providers save time, effort, and costs.
- **Secure:** The security is commensurate with the risk (total of 36 controls).

IMPACT

IMPACT

What does this mean for you?

AGENCIES

- An Agency can assist a CSP in completion of required documentation.
- An Agency or 3PAO may perform assessment of implemented controls. The AO can determine degree of required independence.
- An Agency AO must examine the implementation of the system and associated risks to determine security posture and ultimately issue an ATO.
- An Agency can reuse a FedRAMP Tailored authorization from another agency.

3PAOs

- 3PAOs will need to learn the new baseline and adjust their current documentation and processes in alignment with FedRAMP Tailored.
- An Agency may request a 3PAO to perform the assessment of implemented controls.
- Simplifies reviews.

CSPs

- FedRAMP will provide mandatory templates and specific test cases for FedRAMP Tailored for CSPs to utilize.

NEXT STEPS

Initial Feedback

Initial Feedback from Agencies and Industry

- Overall, comments were very positive and there was consensus that a baseline to address these low-risk niche-services is needed.
- There were several hot topics that received the most attention:

  - Non-US persons with development or administrative access
  - What qualifies as PII?
  - Requirement for SaaS to be hosted on a FedRAMP-Authorized IaaS. What about SOC2/PCI, etc?
  - How do CSPs determine is FedRAMP Tailored is the appropriate baseline they should follow?

NEXT STEPS

What are the next steps?

- DRAFT FedRAMP Tailored documentation is currently up on the FedRAMP website: https://tailored.fedramp.gov/
- There was a 60-day Public Comment Period & FedRAMP Tailored Comment-a-thon that closed in May; we received over 300 comments from over 50 different Federal Agencies and Industry groups.
- Please visit the link on the FedRAMP homepage or in our recent blog entitled "Launching a FedRAMP *Tailored* Baseline" and share your feedback with us.
- A second DRAFT version of the documentation will be released this summer accompanied by another round of public comments.

QUESTIONS & FEEDBACK