



Federal Risk and Authorization Management Program

HIGH BASELINE

June 29, 2016 | www.fedramp.gov



HIGH SYSTEM

High impact systems are systems that contain high impact data according to the Federal Information Processing Standard (FIPS) 199.

FIPS 199 categorizes data according to three unique elements

- Confidentiality
- Integrity
- Availability



In simple terms, if any of those elements were impacted, it would pose a severe risk to life, limb, or financial ruin.

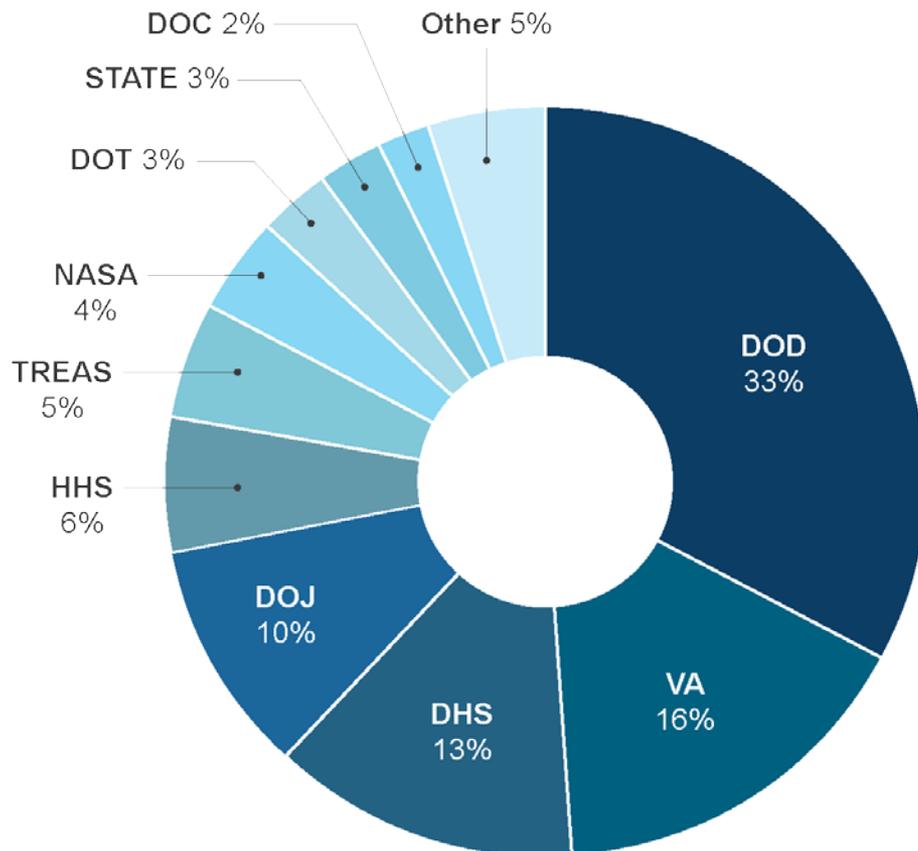
- By definition, this means any impact would have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

Typical high impact systems include:

- Law enforcement systems
- Health systems
- Financial systems



HIGH BASELINE DEMAND

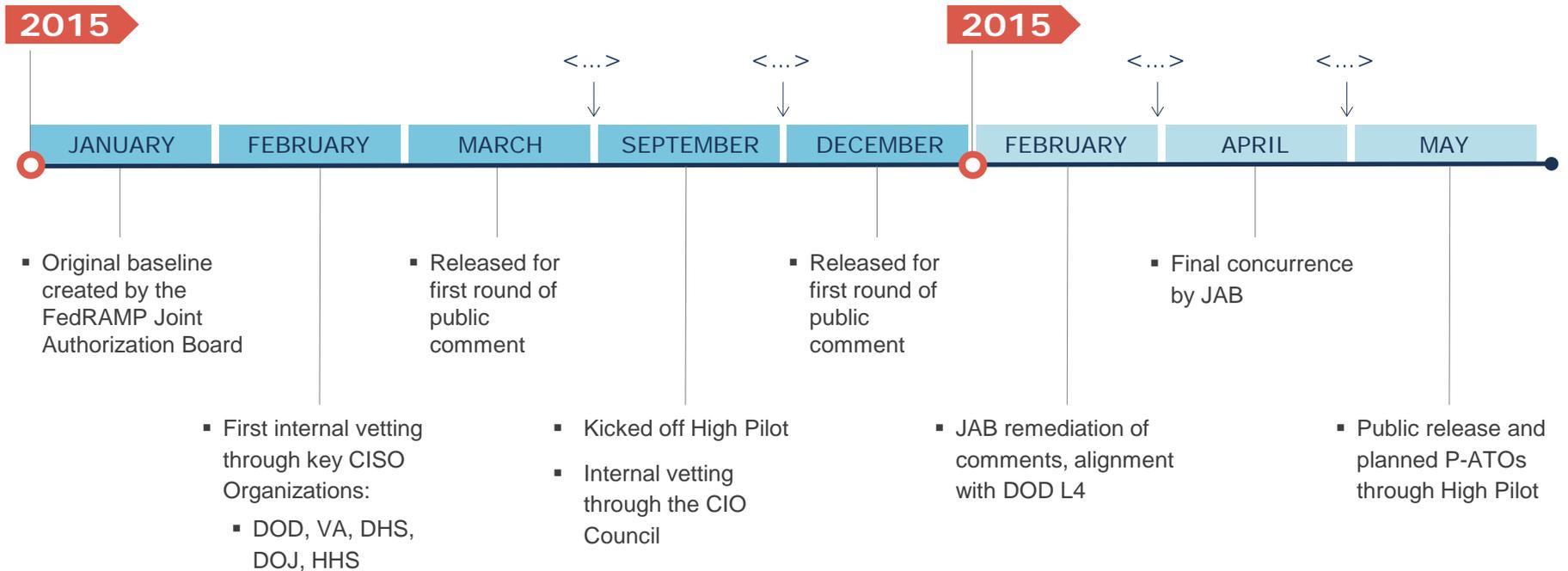


Interest Across FedRAMP's Stakeholders

- Federal Agencies
- State, Local, Tribal
- NIST
- Cloud Service Providers
- Third-Party Assessment Organizations



TIMELINE





Goals of the Pilot

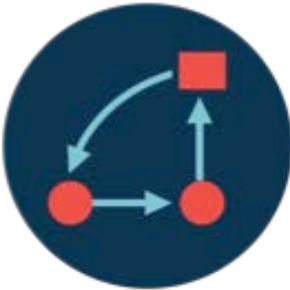
- Determine if the requirements could be implemented by commercial providers
- Ensure requirements weren't academic but based in reality
- Allow agencies to begin using high cloud services immediately upon release of the baseline requirements
- Provide agencies a competitive range of vendors they could begin to use
- Give high system owners the assurance that these systems were secure by validation through the JAB



THE PROCESS

Used the Risk Management Framework (800-37) as applied to low and moderate systems

1. Categorize data
2. Select control
3. Implement
4. Test
5. Authorize
6. Continuously monitor

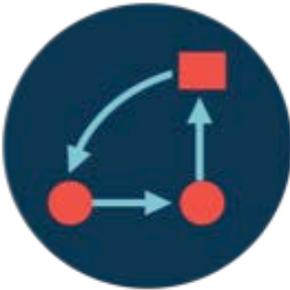


Only difference is the number of controls and implementations

1. **Categorize data** - High impact according to FIPS 199
2. **Select the controls** - New FedRAMP High baseline requirements
3. **Implement** - Implement the totality of the controls in the requirements

In the future, CSPs can use the High Baseline to pursue either JAB P-ATOs or Agency ATOs

- Same process, just looking at additional controls



Efficiencies gained through FedRAMP Accelerated will also apply to high systems pursuing a JAB P-ATO

- The process will be the same; the only difference is the additional controls for high systems.



Key considerations for vendors



Architectural Considerations

- Automation
- MFA with eAuth Level 4 for both government AND privileged CSP users
- FIPS 140-2 encryption issues

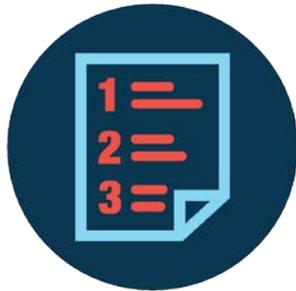


Operational Considerations

- Shared services IN the authorization boundary
- Many enhanced parameters (e.g. lock-out timeframes) and 96 additional controls in Rev 4 high baseline (compared to Rev 4 moderate baseline)



AUTHORIZED HIGH SYSTEMS



Through this process, we've gotten ATOs for three high systems:

- Microsoft Azure Government IaaS/PaaS
- Amazon Web Services GovCloud IaaS
- Autonomic Resources/CSRA ARC-P IaaS



FOR MORE INFORMATION

