FedRAMP

A FEDRAMP **AUTHORIZATION BOUNDARY**

Matt Goodrich

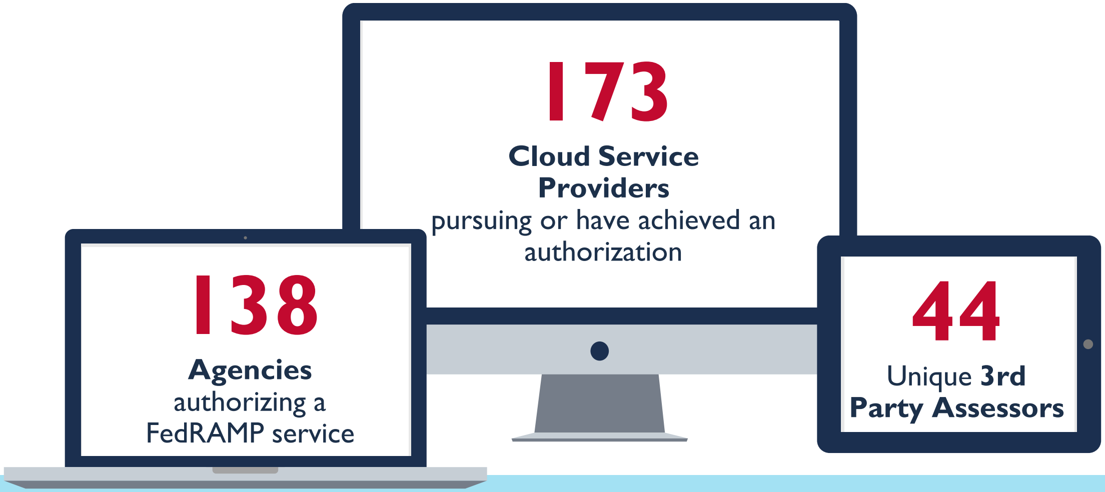
Director, FedRAMP

FedRAMP At A Glance

FedRAMP was created out of the U.S. Government's Federal Cloud Computing Initiative to *remove the barriers* to cloud adoption

FedRAMP's Goals

- Ensure the use of cloud services **protects** federal information
- Enable **reuse** across the Federal government wherever possible to save money and time



173

Cloud Service Providers pursuing or have achieved an authorization

138

Agencies authorizing a FedRAMP service

44

Unique **3rd Party Assessors**

In 6 Years, FedRAMP **Enabled** Government To Avoid

>$168 MILLION IN COSTS

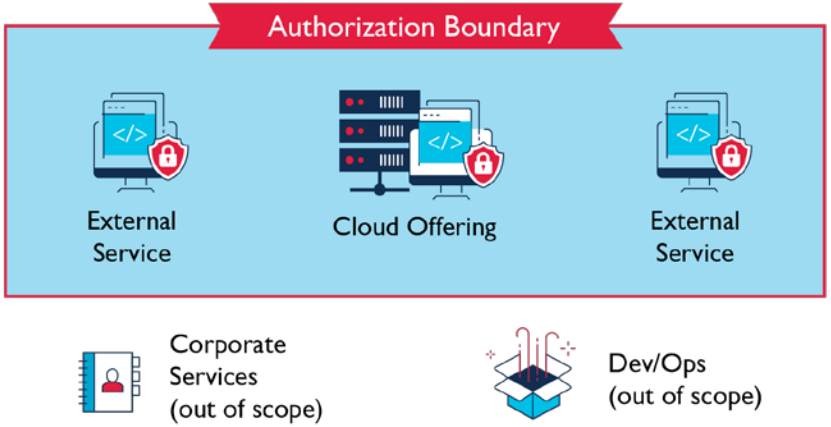
Why FedRAMP Published Guidance

PROBLEM

Cloud Service Providers (CSPs) were having difficulty accurately describing and depicting their authorization boundaries in the cloud from a FISMA perspective for FedRAMP authorization

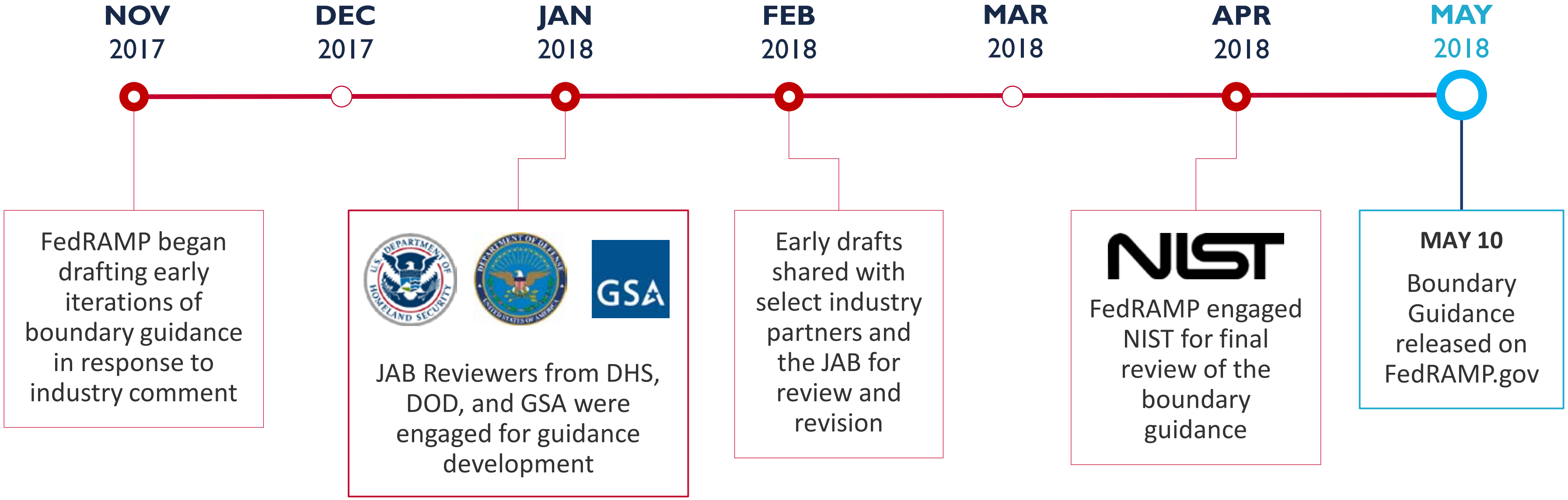
FedRAMP created guidance to:

- Define the key considerations that should be accounted for by CSPs when describing and depicting their authorization boundaries
- Inform CSP's preparation and architecture development for FedRAMP authorization
- Educate industry and agency partners on expectations for boundary demonstration in security documentation



Timeline – Creating the Guidance

Boundary guidance was created in coordination with the
Joint Authorization Board (JAB), NIST, and our **trusted industry partners**



NOV 2017

FedRAMP began drafting early iterations of boundary guidance in response to industry comment

DEC 2017

JAN 2018

JAB Reviewers from DHS, DOD, and GSA were engaged for guidance development

FEB 2018

Early drafts shared with select industry partners and the JAB for review and revision

MAR 2018

APR 2018

FedRAMP engaged NIST for final review of the boundary guidance

MAY 2018

MAY 10

Boundary Guidance released on FedRAMP.gov

Key Concepts: FedRAMP Guidance

Defining an Authorization Boundary in the Cloud	An authorization boundary should: • Describe a cloud system's internal components and connections to external services and systems • Account for the flow of all federal information and metadata • Illustrate a CSP's scope of control over the system • Identify system components or services that are leveraged from external services or controlled by the customer
Federal Information (Data) in the Cloud	• The authorization boundary should include and account for all federal data populated or generated by a federal customer, including metadata
Metadata Associated with the Cloud	Metadata should be accounted for, adequately protected, and documented by the CSP within applicable FedRAMP deliverables. Metadata includes: • Data that describes or imparts information about data populated by a federal customer • Information that could impact the system's confidentiality, integrity, and availability (CIA) included in logs, audit trails, and vulnerability reports
Interconnections in the Cloud	• Cloud technologies utilize interconnections, Application Programming Interfaces (APIs), and other synchronous / asynchronous connections that potentially transmit federal data and metadata • These connections, and any potential risk to federal information, should be disclosed to the Authorizing Official via the FedRAMP deliverables
External Services in the Cloud	• CSPs that leverage external services that are not directly controlled by the vendor pursuing a FedRAMP authorization must clearly communicate these external services to the AO and the extent to which federal information can be impacted by the use of these services • CSPs should make sure their FedRAMP Authorization Package reflects this information
Leveraging External Services with a FedRAMP Authorization	• If a Cloud Service Offering (CSO) is utilizing an external service that has a FedRAMP Authorization, the CSP may demonstrate compliance with various FedRAMP/NIST SP 800-53 control requirements by leveraging these capabilities from another provider • CSPs must reflect this relationship within the FedRAMP Authorization Package
Corporate Services	• These are services that are used by a CSP to support their daily business operations and exist outside of the cloud offering authorization boundary. These services do not contain any information that would impact the CIA of the CSO

Getting Started

Understanding System Data Flows & Interconnections

FedRAMP recommends that CSPs **illustrate the various data flows** within their service offering to inform their authorization boundary

DATA FLOWS TO UNDERSTAND

- Federal Customer User Authentication Logical Data Flow
- Administrative and Support Personnel User Authentication Logical Data Flow
- System Application Data Flow within the proposed boundary
- System Application Data Flow to all Leveraged and Interconnected Systems

Inside the Boundary

Rules of Thumb 1 & 2

RULE OF THUMB 1

Federal Information that is processed, stored, or transmitted by or for the Federal Government, in any medium or form

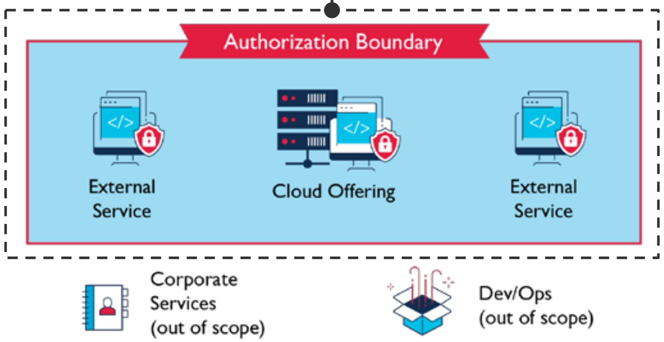
- CSPs are expected to conduct their own due diligence in defining their FedRAMP authorization boundary to identify all instances where federal information is processed, stored, or transmitted
- The authorization boundary should clearly delineate between internal and external services within the CSP's scope of control over the CSO, services that are leveraged from an external provider, and the scope of control of anticipated customer authorization boundaries within the CSO
- The CSP must make the authorization boundary transparent to the Third Party Assessment Organization (3PAO) and the AO. FedRAMP requirements (documentation, testing, continuous monitoring, etc.) apply to all system components that are outlined within the authorization boundary

RULE OF THUMB 2

External services that impact the CIA of federal information

- Any external service that contains federal information or metadata that affects the CIA of federal information within a CSO must be depicted within the boundary
- The CIA impact level is commensurate with a federal customer's required impact level of the data within the CSO as defined by FIPS 199
- External services must be transparent to the AO, to include potential impacts to federal information
- External services that are not FedRAMP Authorized must have an appropriate scope of assessment as determined by the AO's risk tolerance

Rules of Thumb 1 & 2 are associated with the system components that are ***included within an authorization boundary***



Outside the Boundary
Rules of Thumb 3 & 4

RULE OF THUMB 3

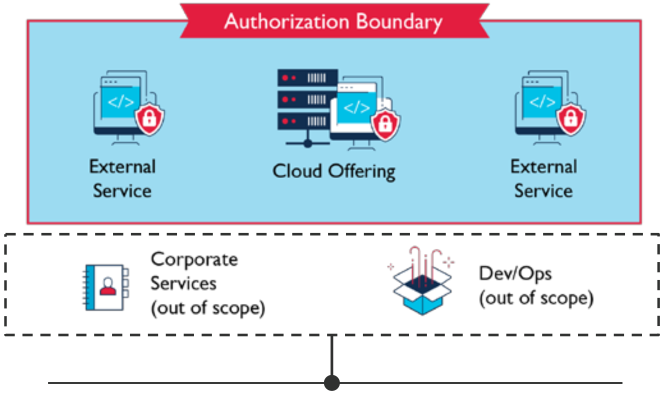
Corporate services that do not affect the CIA of federal information

- CSPs may utilize corporate services such as customer relationship management, ticketing, and billing systems as part of normal business operations
- If data being transmitted in these systems – in line with **Key Concepts #2 & #3** – does not affect the CIA of federal information, these services may be excluded from the authorization boundary
- **Examples of Corporate services outside of the authorization boundary**
  - Customer Relationship Management (CRM) that includes data pertaining to customer relationships only

RULE OF THUMB 4

Development environments that do not process, store, or transmit federal information

- Development environments may be used to design, develop, test, and deliver software and code to end users
- These environments - in line with **Key Concept #2 -** may be excluded from the authorization boundary if there is no federal information within the environment
- Interconnections – in line with **Key Concept #4** – that exist between the development environment and the authorization boundary must be transparent and provided to an AO for review and risk acceptance
- An AO could request the development environment be included within the authorization boundary



Rules of Thumb 3 & 4 are associated with the system components that are typically ***outside an authorization boundary***

Additional Considerations

Agency-specific Security Requirements

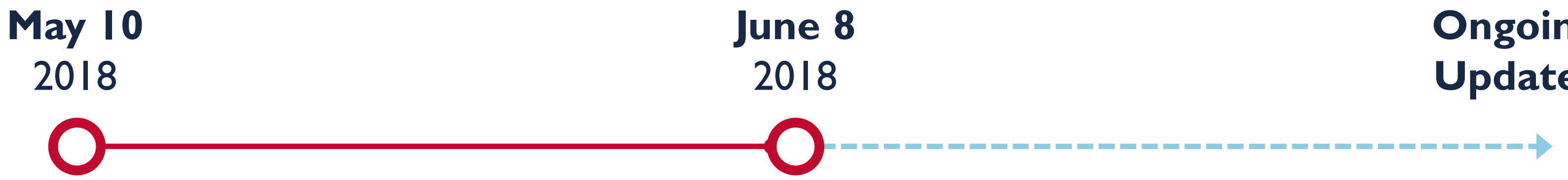
FedRAMP provides a **baseline** from which CSPs and Agencies can define their desired security posture according to FISMA requirements and NIST categorizations

FedRAMP strongly encourages partnership among CSPs and Agencies to determine:

- Additional mission-specific security controls for cloud systems (e.g., privacy controls, controls affected by foreign nationals)
- Additional requirements for federal data types and the impact on a system's cloud authorization boundary

In fulfillment of our mission, FedRAMP facilitates these discussions with CSPs and Agencies to address additional security requirements

Next Steps



FedRAMP is accepting comments on the published boundary guidance from industry and government partners through
Friday, June 8th

Please provide comments to info@fedramp.gov

This resource will continue as a ***living document*** - evolving with changes to cloud computing technology and relevant federal information security policy

QUESTIONS?

Learn more at FedRAMP.gov

Contact us at info@fedramp.gov

@FedRAMP