Overview of the Federal Risk and Authorization Management Program (FedRAMP)

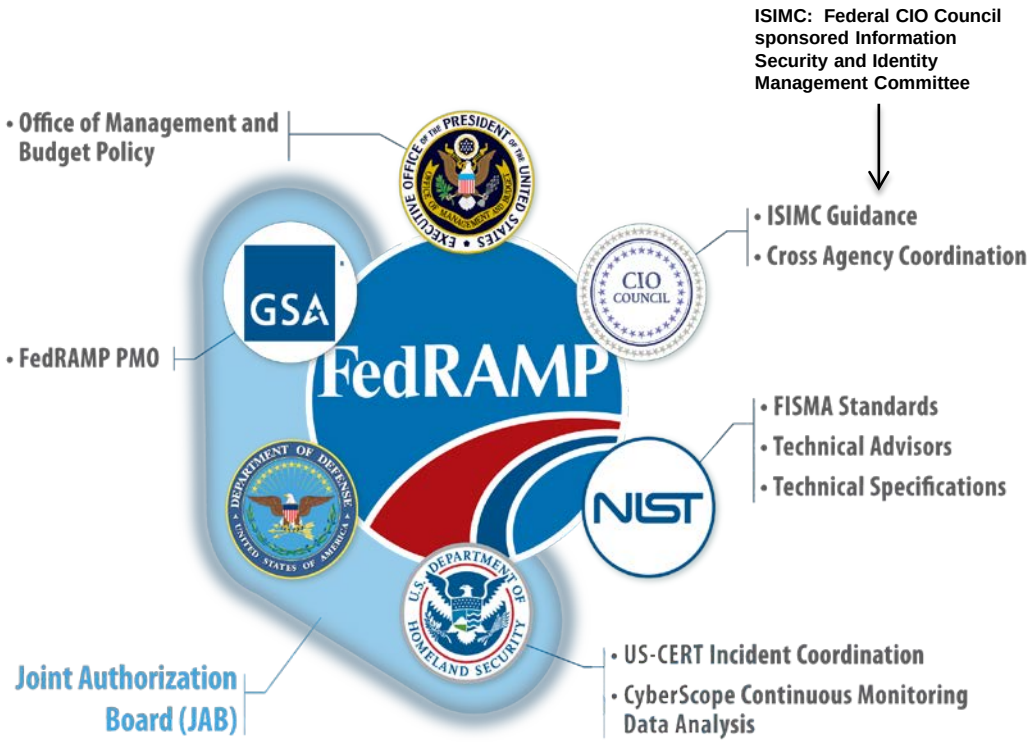
briefing for
Visiting Committee on Advanced Technology (VCAT)

Chuck Romine, Director, ITL

February 8, 2012

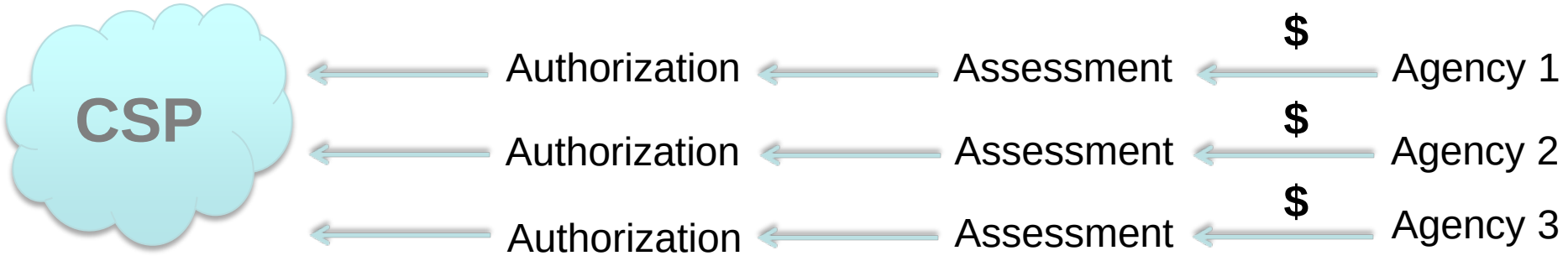
FedRAMP

- Government-wide program
  - OMB Policy Memo (12/8/2011)
  - For cloud products and services
- Provides a standardized approach
  - security assessment
  - authorization
  - continuous monitoring
- Re-uses existing security assessments across agencies

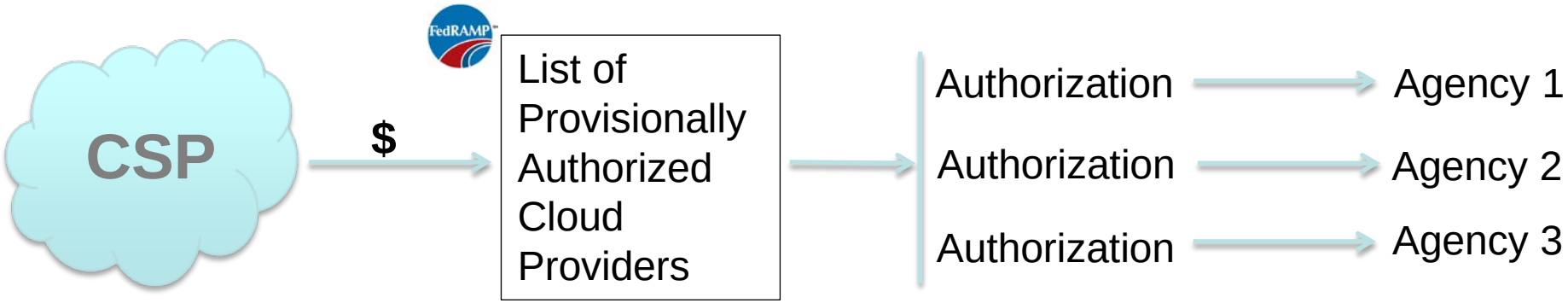


Assess once; Use many

Current Assessment /Authorization Model Applied to Cloud



FedRAMP Model



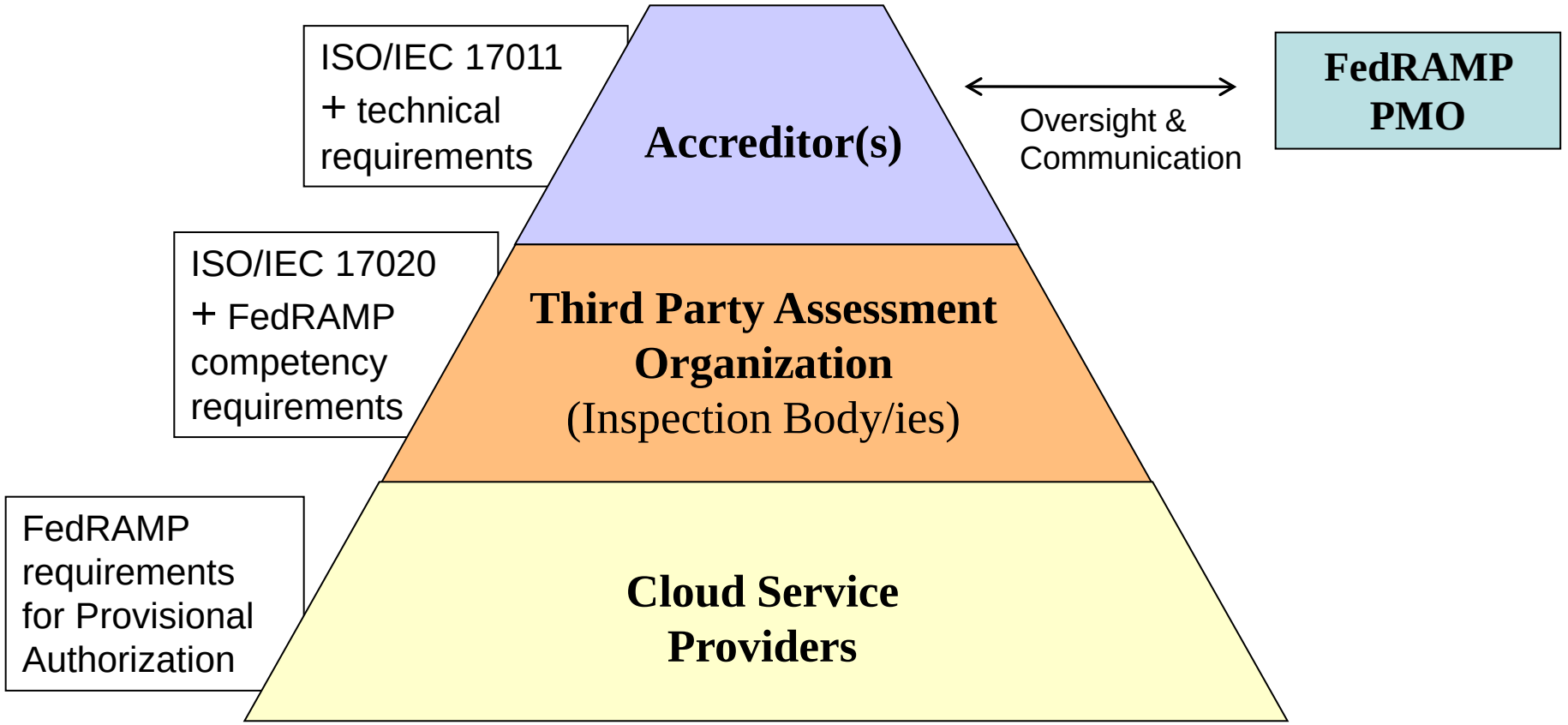
Note: Difference between FedRAMP standard control set and FedRAMP set can be accommodated.

NIST Role

- NIST Cloud Computing Program: build a U.S. Government Cloud Computing Roadmap
- Technical Advisor on FedRAMP
  - Collaborated with Federal CIO Council Security Working Group to develop FedRAMP concept
  - Collaborate with GSA to develop and implement a formal conformity assessment program

    consistent independent, third-party assessments of security controls implemented by Cloud Service Providers
  - Technical Experts regarding FISMA compliance
    - Special Publications (SP) 800-53 and 800-37
    - Federal Information Processing Standards (FIPS) 199 and 200
  - Advise Joint Authorization Board on compliance requirements

FedRAMP Program Built on International Standards



ISO/IEC 17011; Conformity assessment -- General requirements for accreditation bodies accrediting conformity assessment bodies
ISO/IEC 17020; General criteria for the operation of various types of bodies performing inspection

FedRAMP Phases and Timeline

Phased evolution towards sustainable operations allows for risk management, capture of lessons learned, and incremental rollout.

	FY12 Pre-Launch Activities	FY12 Initial Operational Capabilities (IOC)	FY13 Q2 Full Operations	FY14 Sustaining Operations
	Finalize Requirements and Documentation in Preparation of Launch	*Launch IOC with Limited Scope and Cloud Service Provider (CSP)s*	*Execute Full Operational Capabilities with Manual Processes*	*Move to Full Implementation with On-Demand Scalability*
Key Activities	• Publish FedRAMP Requirements (Security Controls, Templates, Guidance) • Publish Agency Compliance Guidance • Accredit 3PAOs • Establish Priority Queue	• Authorize CSPs • Update CONOPS, Continuous Monitoring Requirements and CSP Guidance	• Conduct Assessments & Authorizations • Scale Operations to Authorize More CSPs	• Implement Electronic Authorization Repository • Scale to Steady State Operations
		Gather Feedback and Incorporate Lessons Learned		
Outcomes	• Initial List of Accredited 3PAOs • Launch FedRAMP into Initial Operating Capabilities	• Initial CSP Authorizations • Established Performance Benchmark	• Multiple CSP Authorizations • Defined Business Model • Measure Benchmarks	• Authorizations Scale by Demand • Implement Business Model • Self-Sustaining Funding Model Covering Operations • Privatized Accreditation Board

http://FedRAMP.gov