Building a Cloud Security Authorization (ATO) Strategy

Presented by:

Jaime Lynn Noble, CAP, CISSP
Chief Information Security Officer
Office of Justice Programs
U.S. Department of Justice
Cloud is Here

- Cloud has become an integral part of the Enterprise
  - A catalyst for Business Innovation
  - Driving IT Modernization

$112 Billion Investment In the next 5 years

Cloud is over taking On-Premises

Changing the IT Business

New Skills
• Cloud Adoption Strategy

• Inform Analysis of Alternatives

• Integrate Security into IT Governance
Managing risk is a complex, multifaceted activity that requires the involvement of the entire agency—

- **Senior leaders and Executives** providing the strategic vision and top-level goals and objectives for the agency;
- **Mid-level leaders** planning, executing, and managing projects;
- **Individuals** on the front lines operating the information systems supporting the agency’s missions or business functions.
Cloud Adoption Roadmap

- Understand your Organization’s Mission
  - Drive business value
  - Protect the mission!
- Inform Organizational Cloud Strategy
  - Budget for security
  - Schedule
  - Resources
Cloud Adoption Roadmap
Inform Analysis of Alternatives

• Inform Acquisition Language
  • OMB A-130
    • FISMA requires each agency to provide information security for the information and “information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, and cloud-based solutions.
  • Agency Specific clauses
    • Breach Notification Procedures
    • Disposal of Agency Information
    • FedRAMP
Inform Analysis of Alternatives

- All Cloud Service Providers are not equal
  - Leverage FedRAMP Market Place
  - Sponsor a CSP through FedRAMP
Integrate Information Security

• IT Investment Review Boards
• Enterprise Architecture
  • Common Technologies
  • Reduce complexity
• Systems Development Life-Cycle
  • Budget
  • Acquisitions
  • Security Requirements
Security Assessment & Authorization

Governance

CATEGORIZE
Information Systems
FIPS 199/SP 800-60

RISK MANAGEMENT
FRAMEWORK
Security Life Cycle

SELECT
Security Controls
FIPS 200/SP 800-53

IMPLEMENT
Security Controls
SP 800 Series

ASSESS
Security Controls
SP 800-52A

AUTHORIZE
Information Systems
SP 800-37

MONITOR
Security Controls
SP 800-52A
Information Security Continuous Monitoring

**Governance**

**Federal Agencies**
- Contract with Cloud Service Provider
- Leverage ATO or use FedRAMP Process when authorizing
- Implement Consumer Controls

**FedRAMP PMO & JAB**
- Implement and Document Security
- Use Independent Assessor
- Monitor Security
- Provide Artifacts
- Establish Processes and Standards for Security Authorizations
- Maintain Secure Repository of Available Security Packages
- Provisionally Authorize Systems That Have Greatest Ability to be Leveraged Government-wide

**Cloud Service Provider**
- Cloud auditor, maintains independence from CSP
- Performs initial and periodic assessment of FedRAMP controls
- Does NOT assist in creation of control documentation

**3PAOs**
- Third Party Assessment Organizations
