

Overview of Cloud Computing in the United States

Mark Estberg
Senior Director
Microsoft Corporation
Online Service Security & Compliance



Discussion Topics

- Trends and Observations – Cloud Service Provider Perspective
- U.S. Government Cloud Policy Landscape
- Principles for Government Cloud Security Requirements

Security and Compliance Trends and Observations

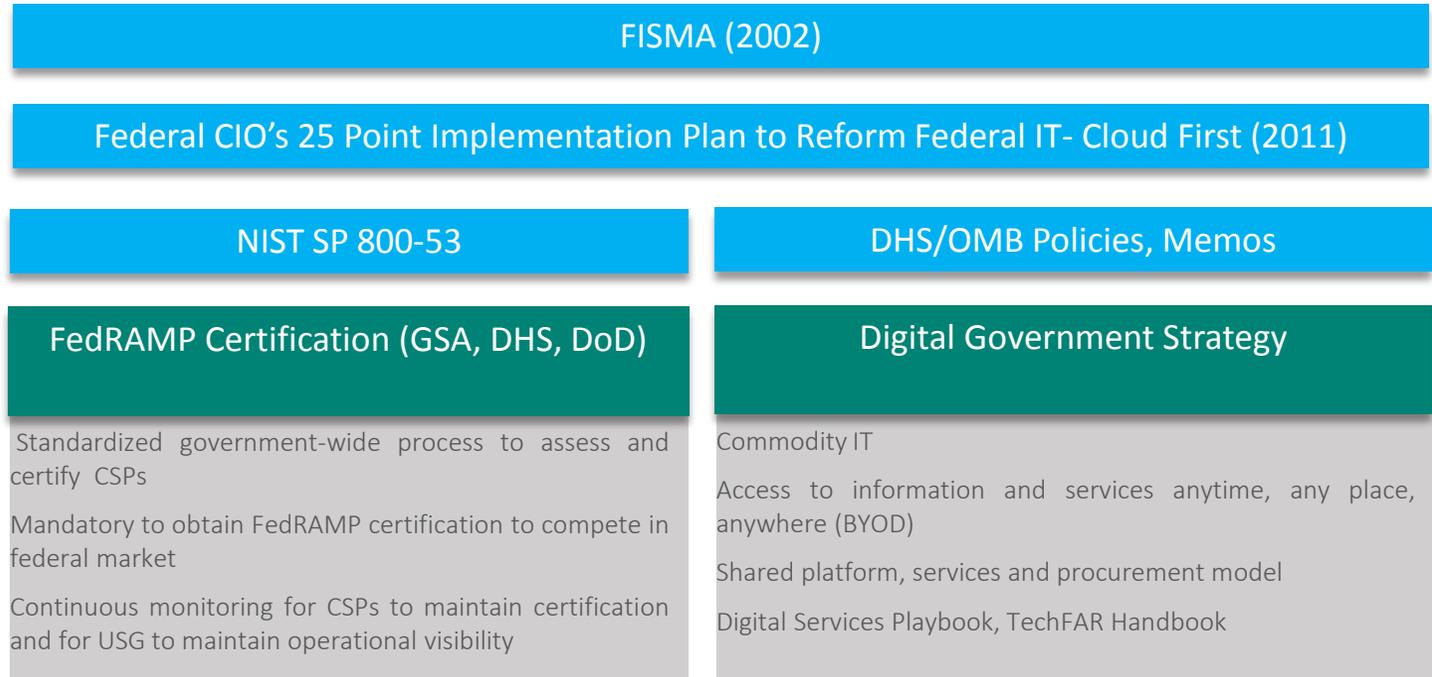
- Legislation and standards proliferation
- Consumer privacy and law enforcement transparency
- Data sovereignty and localization of services
- More persistent and sophisticated attacks
- Cloud and on-premise interoperability
- Changing infrastructure form factors

U.S. Government Cloud Policy Landscape

Controls derived from traditional information security requirements for government systems based on the Federal Information Security and Management Act of 2002.

The U.S. created an overlay of NIST SP 800-53 controls in the cloud and is largely managing cloud security using a similar approach and requirements as in their traditional computing environments.

FedRAMP is a complex cloud risk assessment, authorization and continuous monitoring program that was borne from the USG's goals to advance a more digital, mobile government and workforce.



Principles For Government Cloud Requirements

Certify once,
use many

- Reduces duplication in multiple assessments for the same product or service
- Ensures consistency and repeatability in the evaluation of the security requirements
- Minimizes cost for the service provider and consumer
- Streamlines often times duplicative processes

Risk management,
outcome-focused

- Focus on the desired security outcomes and then determine which practices can deliver those outcomes
- Baseline set of security requirements that systems are certified against need to reflect risk prioritization
- More controls does not equal increased security

Practicable

- Given the complexity of threats, risks, and cloud architectures, ensuring that a certification can actually be obtained without undue concern over a taxing resource burden will be key
- Accessible for small and medium-sized entities who will likely lack the financial and personnel resources to grapple with overly-complex or burdensome requirements, certifications must be practical.
- Feasible for major CSPs given the global scale of their service offerings

Scalable

- Excessive one-off, customer-specific requirements are not scalable and result in costs cascading down to the customer
- Given the scale at which cloud computing is delivered and consumed and its inherent dynamic and agile environment, requirements implementation require flexibility beyond a traditional network environment

Principles For Government Cloud Requirements

Based on global standards

- Reduces duplication in multiple assessments for the same product or service
- Ensures consistency and repeatability in the evaluation of the security requirements
- Minimizes cost for the service provider and consumer
- Streamlines often times duplicative processes

Allows for Innovation

- Prescriptive requirements for specific practices or tooling often inadvertently increase costs for government and industry without actually reducing risk and stifle the innovation necessary to develop technology neutral approaches for countering existing and emerging threats
- Extensible so that developers can build on top of existing platforms to support customers' changing needs

Transparent requirements process

- Enables a comprehensive, well-understood, and easily adoptable compliance framework
- Set expectations from the onset around clarifying the intent of a requirement, reaching consensus on terminology, and determining the technical reasonableness of requirements to preempt unforeseen challenges and avoid additional work cycles or other inefficiencies during the actual certification process

Clear designation of roles and responsibilities

- Align requirements based on cloud-based operations (vs. traditional network environment)
- Clearly define risk ownership (v. control implementation) among CSPs, customer, and other cloud stakeholders (e.g. assessor, broker)