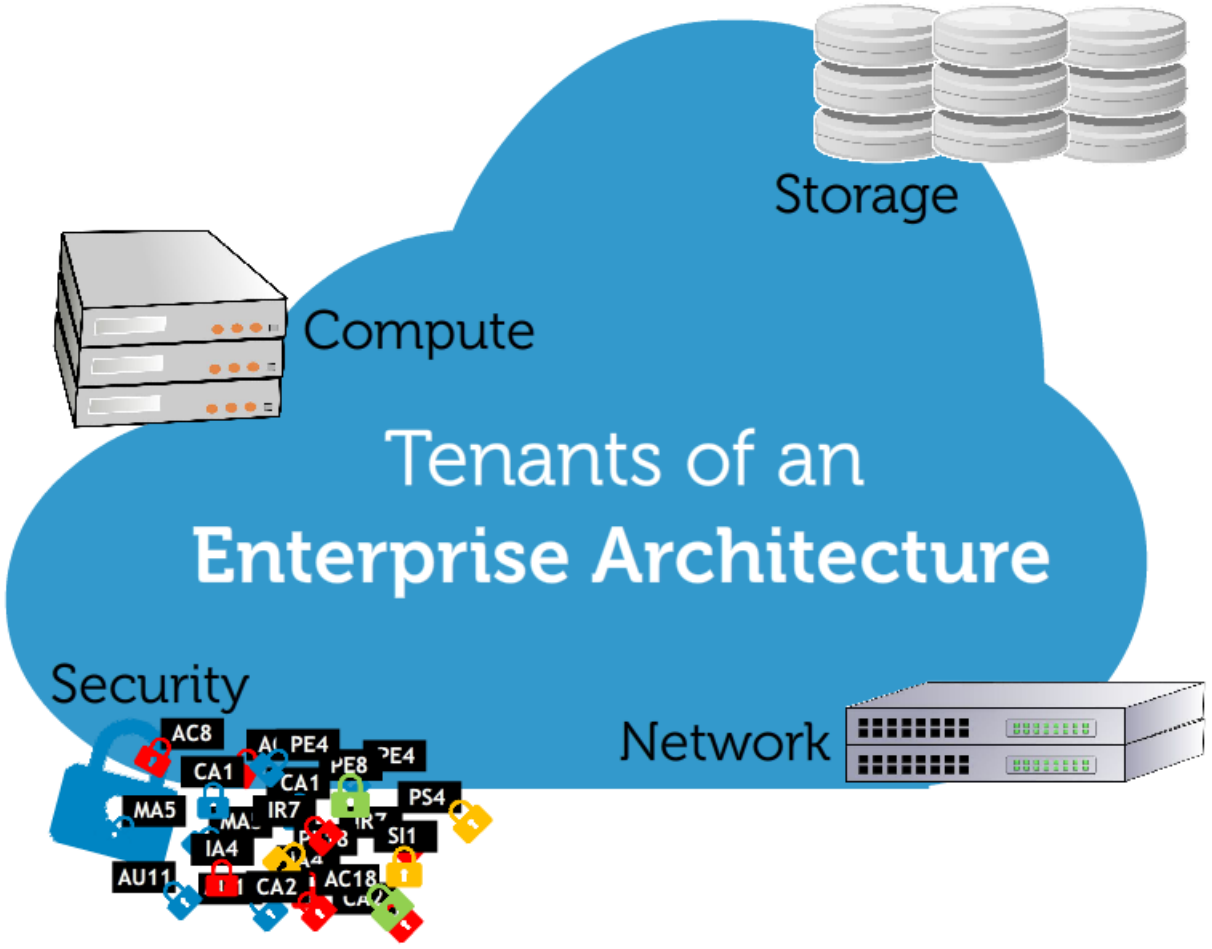
Dell Cloud for US Government (DCG)

Cloud Architecture

Jeffrey Lush
CTO, Dell Services Federal Government
Jeffrey_Lush@federal.dell.com

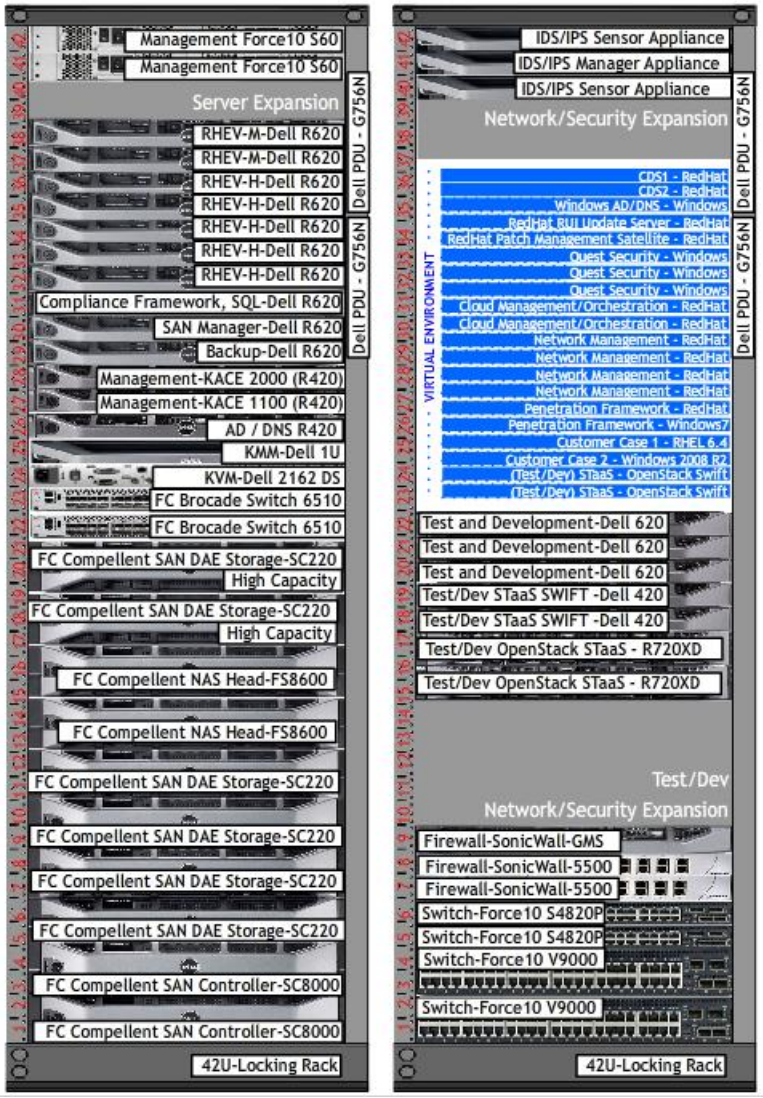
Enterprise strength makes a Cloud functional

Dell Cloud for US Government



- Performance
- Scalability
- Flexible
- Location Agnostic
- Dedicated / Multi-tenant

Dell Cloud for US Government



If you can not manage the ATO effectively, the technology really does not matter

Dell Cloud for US Government

FBI receives their **ATO** that **inherits DCG** FedRAMP controls

+ Security controls are developed to secure EaaS

+ FBI requires EaaS that will reside within the FedRAMP Cloud

STIG NOS Hypervisor

Infrastructure as a Service

NIST 800-53 Controls

FISMA ACT 2002
Infrastructure Security and Process
NIST 800-53 Rev 1-3, FedRAMP, Rev 4

FedRAMP IaaS

ATO Management

REQUIREMENT: Control management of all controls within the FedRAMP environment, dynamically. Validated every 3 months. **OMB requirement: June, 2014**

Continuous Monitoring

REQUIREMENT: Continuous Monitoring of all IP devices. Each device will be touched every 3 days. **OMB requirement: Nov 14, 2014**

Manual - Customer responsibility

Manual tracking each ATO individually

Every 3 months

Security Officer approval

Analyze all 1/3 of all devices and logs daily per ATO

ATO approval

remediation workflow

discover vulnerability

Dell Cloud for US Government

Inherit Controls

Automated collection of tools

Automated Impact Analysis

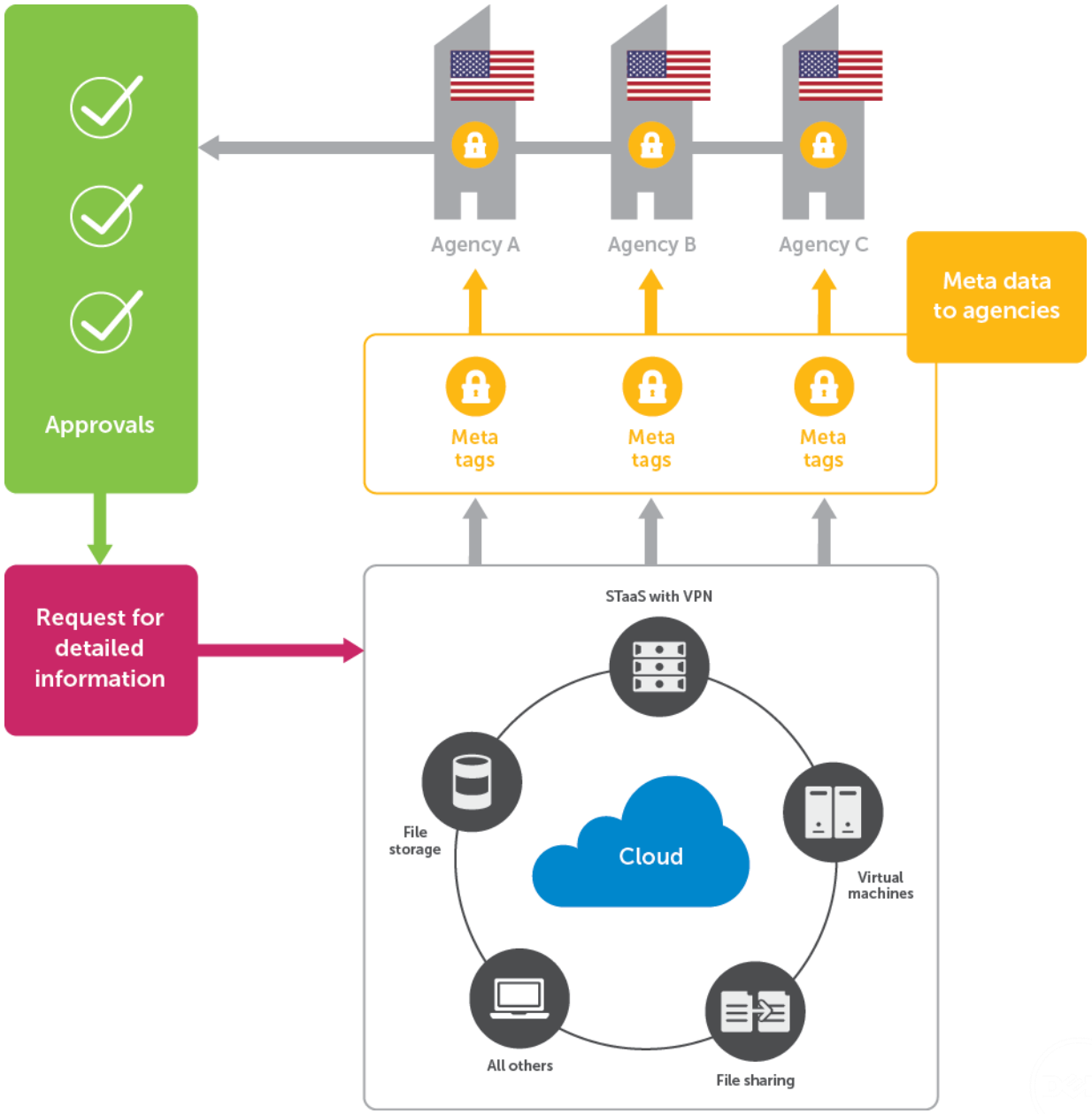
Security Officer approval

Automated Risk Analysis

DCG Compliance Framework

Where will Cloud take us?

Dell Cloud for US Government



Focused on the needs of federally secured environments.

Dell Cloud for US Government

Dell Cloud for U.S. Government

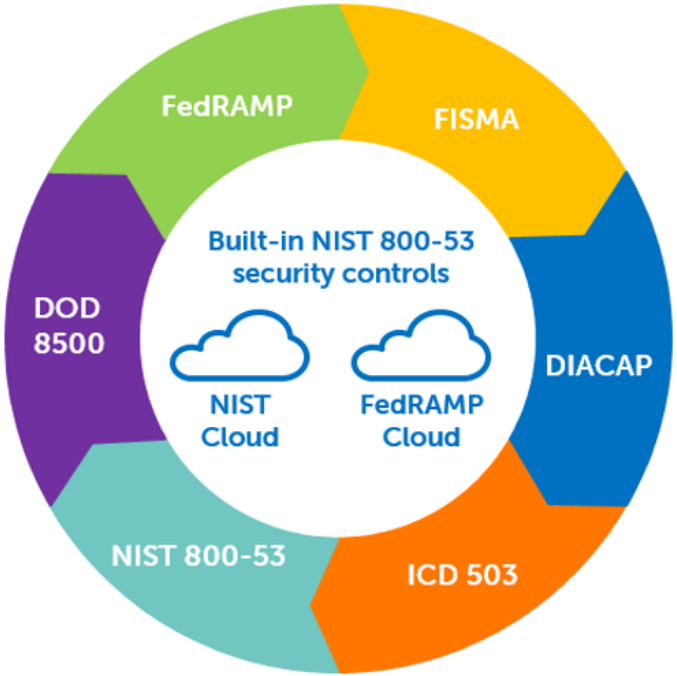
addresses specific agency needs.

NIST Cloud
Dedicated private cloud

Meets special requirements on-site and off-site.

FedRAMP Cloud
Multi-tenant cloud

Safe to share data across environments. Hosted off-site.



Thank you for your time

Dell Cloud for US Government

Jeffrey_Lush@federal.dell.com
512.507.9728