DEFENSE INFORMATION SYSTEMS AGENCY
The IT Combat Support Agency

DOD Cloud Computing

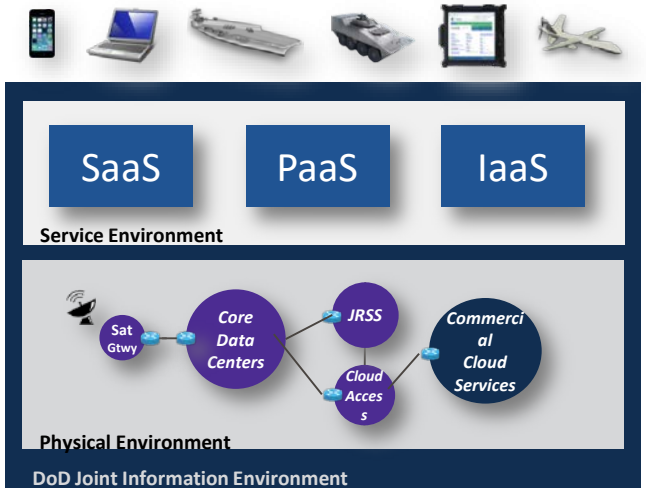
Evolving Capabilities for the Next Generation of Computing

Roger S. Greenwell
Risk Management Executive/
Authorizing Official

15 May 2018

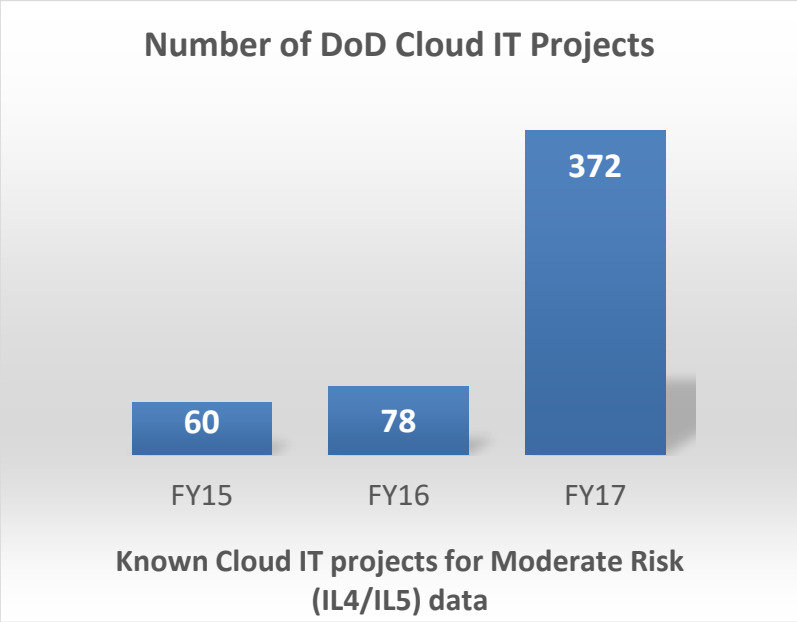
DoD Cloud Vision

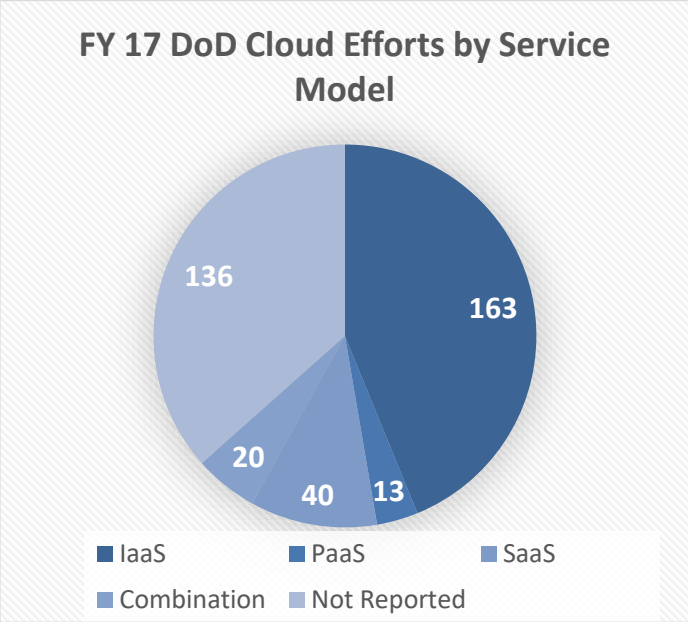
Deliver an assured DoD Cloud Computing Environment capable of responding to the Department's rapidly changing mission needs while improving return on our IT investments.



Deliver commercial cloud capability faster and drive down costs with an acceptable risk-based security posture

Cloud Adoption in DoD is Accelerating





DoD Cloud Trend

Hybrid Enterprise Cloud

(For moderate and high-impact systems)

Building with the Leaders

On-Premise/Private Commercial Clouds

- *Operated within DoD cybersecurity boundary*
- *Integrated with DoD data center and network infrastructure*

Cloud Market Consolidating to the Major Public Clouds

- *Private cloud providers struggle to match innovation and investment of the large public clouds*

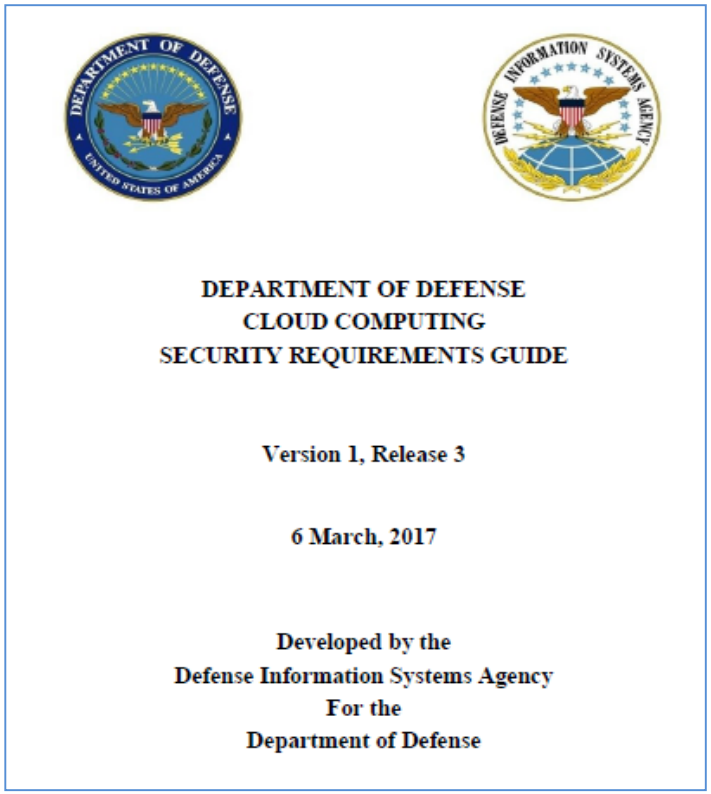
Public Clouds

- *Enhanced to meet DoD cyber requirements*
- *Extending the DoD cybersecurity boundary into external environments*
- *Instantiate private versions for classified and OCONUS systems*

FY 14 FY 15 FY 16 FY 17 FY 18 FY 19

End state envisions a device-to-data centric paradigm shift that will empower information sharing and decision making, driving operational impact, and reducing the cost of DoD IT so that funds can be redirected to operational priorities

Cloud Computing SRG v1r3



DEPARTMENT OF DEFENSE
CLOUD COMPUTING
SECURITY REQUIREMENTS GUIDE

Version 1, Release 3

6 March, 2017

Developed by the
Defense Information Systems Agency
For the
Department of Defense

Table of Contents

PA & ATO Terminology

FedRAMP Provisional Authorization (PA)

- Issued by the FedRAMP Joint Authorization Board (JAB) to a Cloud Service Provider (CSP) for their Cloud Service Offering (CSO)

DoD PA – Will typically reuse (inherit) a CSP's JAB PA (or Federal Agency ATO)

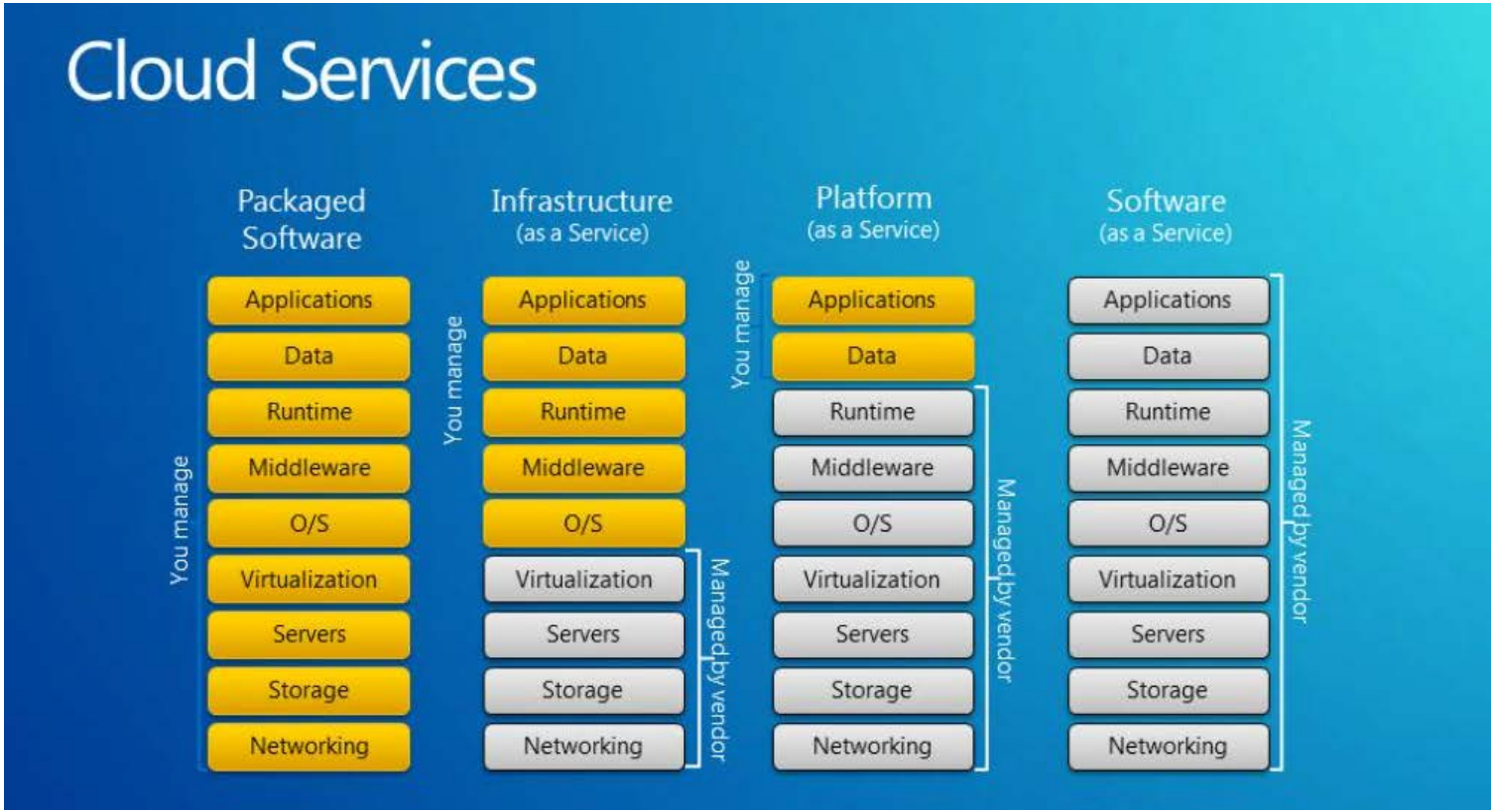
- Issued by the DISA Authorizing Official (AO) to a CSP for their CSO, based on additional DoD security requirements (Levels 4/5/6)
- A DoD PA Level 2 will be issued via reciprocity for approved FedRAMP JAB and Agency PATO

DoD Authorization to Operate (ATO) – Will leverage a CSP's DoD PA

- Issued by a DoD Component AO to a Mission Owner (MO) for their system that makes use of the CSP's CSO

PA – Focuses on CSO Risk	ATO – Focuses on Mission Risk
Granted by: The FedRAMP JAB and the DISA AO To: A CSP for their CSO	Granted by: A DoD Component's AO To: A DoD Mission Owner for their system

Shared Responsibility for Security

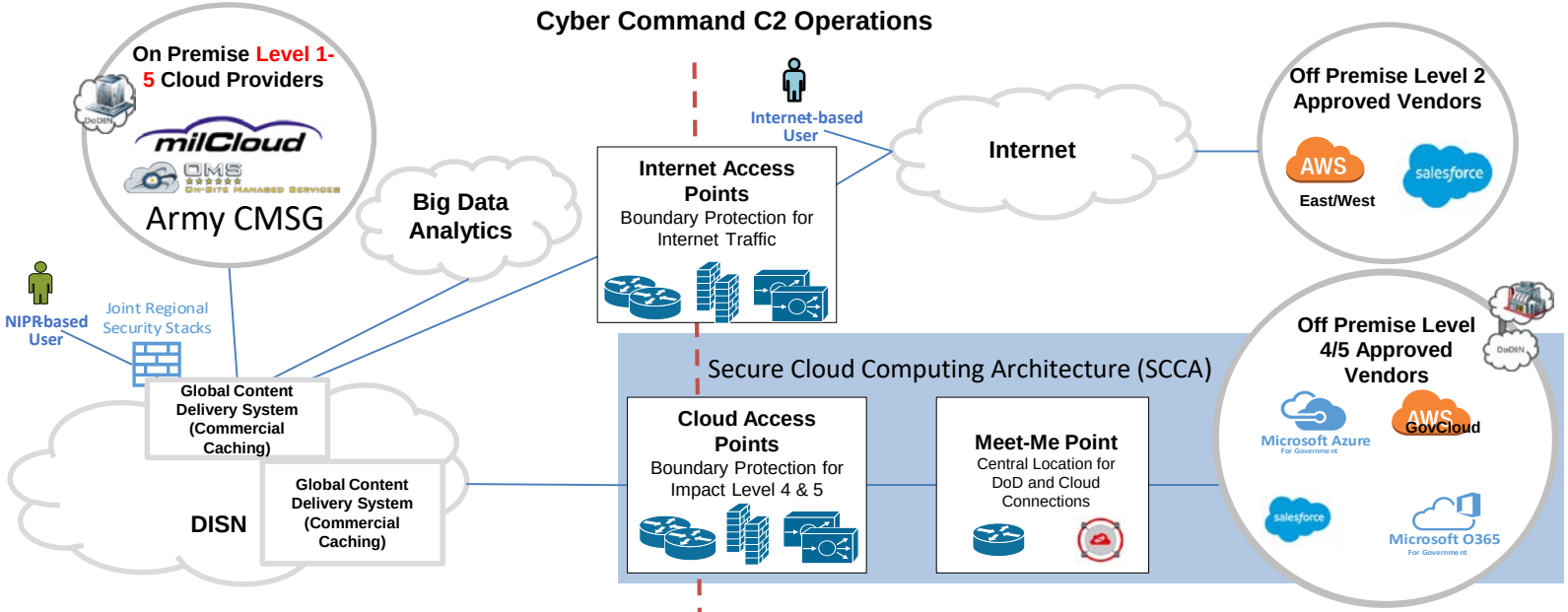


Impact Levels

FedRAMP's Baseline and Impact Level

IMPACT LEVEL	INFORMATION SENSITIVITY	SECURITY CONTROLS	LOCATION	OFF-PREMISES CONNECTIVITY	SEPARATION	PERSONNEL REQUIREMENTS
2	PUBLIC or Non-critical Mission Information	FedRAMP v2 Moderate	US / US outlying areas or DoD on-premises	Internet	Virtual / Logical PUBLIC COMMUNITY	National Agency Check and Inquiries (NACI)
4	CUI or Non-CUI Non-Critical Mission Information Non-National Security Systems	Level 2 + CUI-Specific Tailored Set	US / US outlying areas or DoD on-premises	NIPRNet via CAP	Virtual / Logical Limited "Public" Community Strong Virtual Separation Between Tenant Systems & Information	US Persons ADP-1 Single Scope Background Investigation (SSBI)
5	Higher Sensitivity CUI Mission Critical Information National Security Systems	Level 4 + NSS & CUI-Specific Tailored Set	US / US outlying areas or DoD on-premises	NIPRNet via CAP	Virtual / Logical FEDERAL GOV. COMMUNITY Dedicated Multi-Tenant Infrastructure Physically Separate from Non-Federal Systems Strong Virtual Separation Between Tenant Systems & Information	ADP-2 National Agency Check with Law and Credit (NACLC) Non-Disclosure Agreement (NDA)
6	Classified SECRET National Security Systems	Level 5 + Classified Overlay	US / US outlying areas or DoD on-premises CLEARED / CLASSIFIED FACILITIES	SIPRNET DIRECT With DoD SIPRNet Enclave Connection Approval	Virtual / Logical FEDERAL GOV. COMMUNITY Dedicated Multi-Tenant Infrastructure Physically Separate from Non-Federal and Unclassified Systems Strong Virtual Separation Between Tenant Systems & Information	US Citizens w/ Favorably Adjudicated SSBI & SECRET Clearance NDA

Unclassified DoD Commercial Cloud Deployment Approach



Cloud Acquisition Guidance

Standard Contract Clauses and Provisions

DFARS SUBPART 239.76: Cloud Computing

- Applicability: Commercial cloud services used by or provide on behalf of the Department
- Requires: Cloud provider to meet and maintain DoD Cloud Computing Security Requirements Guide (CC SRG)
- Specifies: Cyber Incident response procedures, data ownership and management requirements, and hosting within the United States

DoD Cloud Contracting Guidance

Defense Acquisition Guidebook (DAG), Chapter 6.3.9.2

- Cloud Computing Definition
- Understanding DoD Cloud Policies
- Information and actions required for DoD Program Managers
- Cloud Computing Service Level Agreements (SLA) Guidance

Addressing DoD's Cloud Challenges

Define and publish DoD cybersecurity requirements

- Cloud Computing Security Requirements Guide (CC SRG)
- On-going technical exchanges with industry partners to advance cloud security
- DFARS requirement established for protection of information in the cloud

Protect the DoD Information Network (DoDIN)

- Over 90 DoD Provisional Authorizations issued to commercial clouds
- Collaboration with FedRAMP for continuous monitoring and on-going assessments

Extend DoD Networks to Commercial Providers

- DISA and Navy Cloud Access Points (CAP) deployed
- Commercial Meet-me points in place to support DoD connections to CSP networks
- Connections with IL4/IL5 CSPs: AWS Govcloud, Microsoft O365/Azure, DoD Oracle

DoD Cloud Acquisitions

- On-Prem/Private Cloud: Examples- milCloud v2, On-Prem Managed Services (OMS), Army Private Cloud Enterprise (APCE))
- DoD-Public Cloud: Example - AF Cloud Hosted Enterprise Services (CHES)

In Place Today

Securing DoD Data Hosted in the Cloud

- DISA and Army Research Labs (ARL) Cybersecurity Support Services
- DoD Secure Cloud Computing Architecture

Emerging

Cloud Cybersecurity Focus

Identity and Access Management (IdAM)

- Support for CAC authentication or other high assurance authentication methods is limited
- Strong authentication for privileged users can be a challenge

Protecting DoD Data in the Cloud

- The Department's ability to protect its data and respond to cyber incidents is maturing
- DoD working with the CSPs to deploy new tools and techniques for enhance capabilities (e.g. Secure Cloud Computing Architecture [SCCA] capabilities)
- CSSP Services to support defense of systems and data in the Cloud

Secure Connections to the Cloud

- Communications with mission critical off-premise cloud providers requires reliable and appropriately secure communications with capacity to support mission needs
- DISA is actively deploying the next generation DoD CAP
- DoD working with industry on other potential approaches for commercial CSP connectivity

Cybersecurity Assessments

- The growing number of CSPs and their on-going delivery of new services creates an assessment challenge
- Leveraging FedRAMP and 3rd Party Assessors (3PAOs) to support assessment process; partnership across the DoD community to assess and monitor CSP activities

Tracking DoD Cloud Efforts

DoD Budget Reporting

Select & Native Programming Data Input System for Information Tech. (SNaP-IT)

- Authoritative source for publishing DoD Budget Estimates
- Updated to collect cloud computing and cloud migration budget information

Cloud Computing Implementations

Systems/Network Approval Process (SNAP) System

- Official system for managing DoD network connections
- New modules deployed in SNAP to manage connections to commercial clouds
- Provides management and visibility into runtime cloud use within DoD
- Critical to situational awareness of where data/systems are located in the cloud

Cloud Computing Cybersecurity Assessments

Enterprise Mission Assurance Support Service (eMASS)

- DoD's tool supporting implementation of the DoD Risk Management Framework
- Extensions being developed to enable CSPs to manage their cyber assessments
- Support accelerated Authority to Operate (ATO) process

Official systems for managing DoD IT are being updated to track and manage DoD cloud computing efforts

Summary

- Cloud services will be a critical component of the Department's Joint Information Environment
- The Department's adoption of commercial cloud services is accelerating, but challenges remain
- DoD is working with industry to:
  - Improve our cybersecurity posture
  - Provide assured network connectivity
  - Enable DoD to better protect its data in the cloud
- Migrating legacy DoD systems to the cloud will be a challenge
  - Rationalizing and consolidating the disparate legacy environment
  - Reengineering or reconfiguring systems for the cloud

DoD must continue to be a smart user of commercial technology, innovate at the speed of relevancy, and improve lethality – moving to the cloud is a critical enabler

DEFENSE INFORMATION SYSTEMS AGENCY
The IT Combat Support Agency

www.disa.mil **/USDISA** **@USDISA**