DEFENSE INFORMATION SYSTEMS AGENCY
The IT Combat Support Agency

Welcome to the

DISA Cloud Symposium

Vendors named within are approved or under contract to provide specified services to DISA or DOD

DEFENSE INFORMATION SYSTEMS AGENCY
The IT Combat Support Agency

UNITED IN SERVICE TO OUR NATION

Vendors named within are approved or under contract to provide specified services to DISA or DOD

Information

Vendors named within are approved or under contract to provide specified services to DISA or DOD

- **IN PERSON VIA QUESTION FORMS, SUBMITTED DURING BREAKS**
- **VIRTUAL INFORMATION PORTAL:**

  http://www.disa.mil/newsandevents/events/cloud-symposium

DISA CLOUD SYMPOSIUM

Vendors named within are approved or under contract to provide specified services to DISA or DOD

DEFENSE INFORMATION SYSTEMS AGENCY
The IT Combat Support Agency

UNITED IN SERVICE TO OUR NATION

Vendors named within are approved or under contract to provide specified services to DISA or DOD

DEFENSE INFORMATION SYSTEMS AGENCY
The IT Combat Support Agency

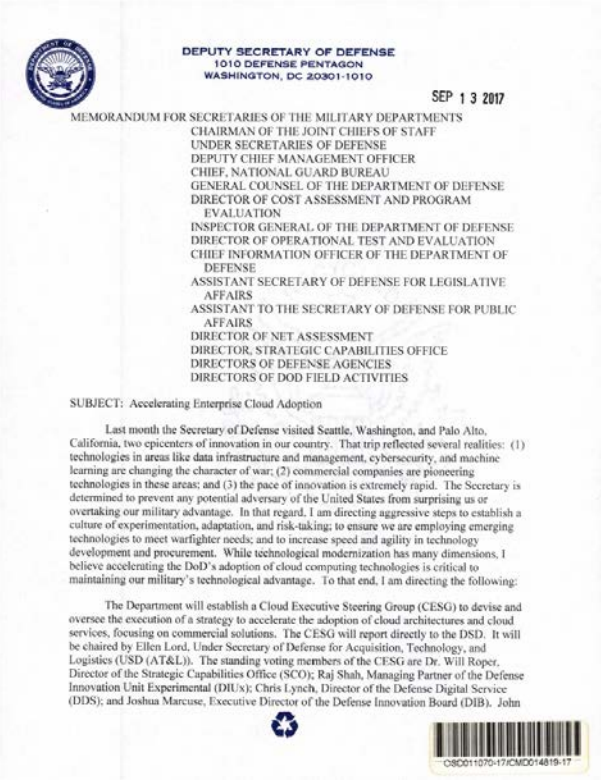
Crawl - Cloud Intro

Mr. John Hale
Chief, DISA Cloud Portfolio
November, 2017

Vendors named within are approved or under contract to provide specified services to DISA or DOD

Deputy Secretary of Defense Memo

Vendors named within are approved or under contract to provide specified services to DISA or DOD



DEPUTY SECRETARY OF DEFENSE
1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010

SEP 1 3 2017

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DEPUTY CHIEF MANAGEMENT OFFICER
CHIEF, NATIONAL GUARD BUREAU
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
DIRECTOR OF COST ASSESSMENT AND PROGRAM EVALUATION
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
DIRECTOR OF OPERATIONAL TEST AND EVALUATION
CHIEF INFORMATION OFFICER OF THE DEPARTMENT OF DEFENSE
ASSISTANT SECRETARY OF DEFENSE FOR LEGISLATIVE AFFAIRS
ASSISTANT TO THE SECRETARY OF DEFENSE FOR PUBLIC AFFAIRS
DIRECTOR OF NET ASSESSMENT
DIRECTOR, STRATEGIC CAPABILITIES OFFICE
DIRECTORS OF DEFENSE AGENCIES
DIRECTORS OF DOD FIELD ACTIVITIES

SUBJECT: Accelerating Enterprise Cloud Adoption

Last month the Secretary of Defense visited Seattle, Washington, and Palo Alto, California, two epicenters of innovation in our country. That trip reflected several realities: (1) technologies in areas like data infrastructure and management, cybersecurity, and machine learning are changing the character of war; (2) commercial companies are pioneering technologies in these areas; and (3) the pace of innovation is extremely rapid. The Secretary is determined to prevent any potential adversary of the United States from surprising us or overtaking our military advantage. In that regard, I am directing aggressive steps to establish a culture of experimentation, adaptation, and risk-taking; to ensure we are employing emerging technologies to meet warfighter needs; and to increase speed and agility in technology development and procurement. While technological modernization has many dimensions, I believe accelerating the DoD's adoption of cloud computing technologies is critical to maintaining our military's technological advantage. To that end, I am directing the following:

The Department will establish a Cloud Executive Steering Group (CESG) to devise and oversee the execution of a strategy to accelerate the adoption of cloud architectures and cloud services, focusing on commercial solutions. The CESG will report directly to the DSD. It will be chaired by Ellen Lord, Under Secretary of Defense for Acquisition, Technology, and Logistics (USD (AT&L)). The standing voting members of the CESG are Dr. Will Roper, Director of the Strategic Capabilities Office (SCO); Raj Shah, Managing Partner of the Defense Innovation Unit Experimental (DIUx); Chris Lynch, Director of the Defense Digital Service (DDS); and Joshua Marcuse, Executive Director of the Defense Innovation Board (DIB). John

OSD011070-17/CMD014819-17

- **Sep 13th, 2017 by Deputy Secretary of Defense**
- **Creates the Cloud Enterprise Steering Group (CESG)**
- **Two phase approach**
  - **Phase 1: Resolve acquisition issues around DoD consuming commercial cloud**
  - **Phase 2: "Rapidly transition" DoD Components and/or Agencies to cloud**
- **Creates regular reporting process of status**

What is cloud?

Vendors named within are approved or under contract to provide specified services to DISA or DOD

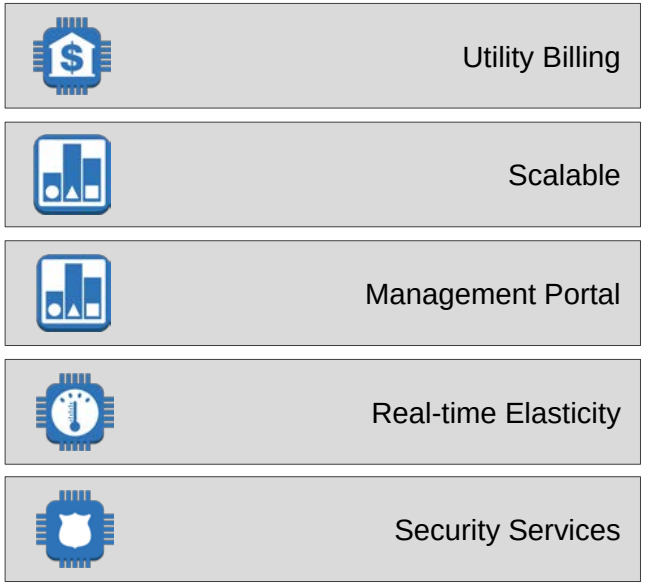
The National Institute of Standards and Technology's (NIST) defines cloud in NIST Special Publication 800-145

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction

What is cloud? (Cont.)

Vendors named within are approved or under contract to provide specified services to DISA or DOD

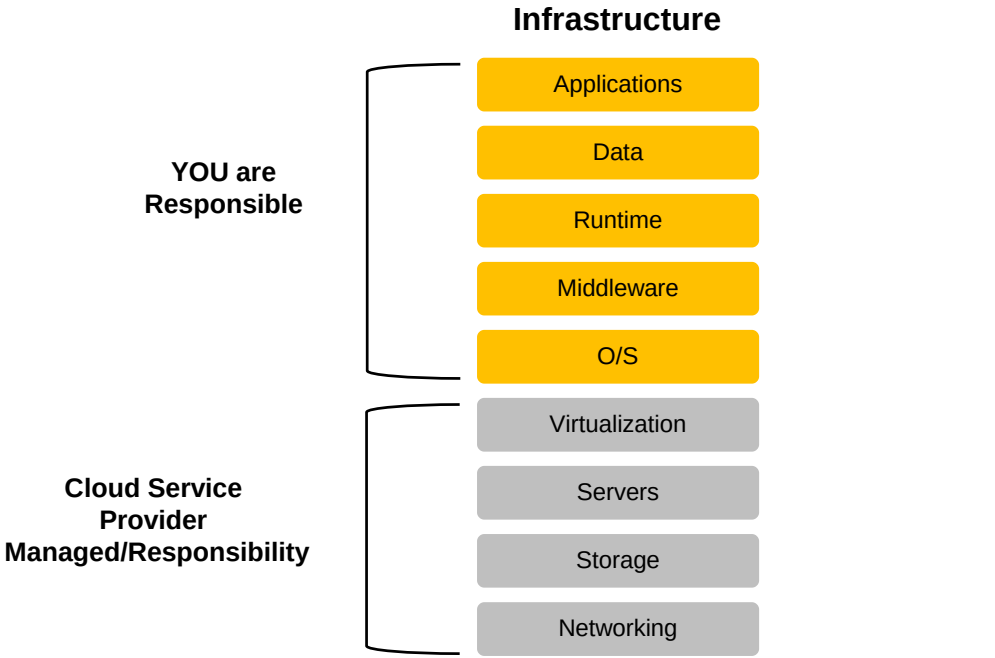
- **In reality, cloud is:**



Cloud Models

Vendors named within are approved or under contract to provide specified services to DISA or DOD

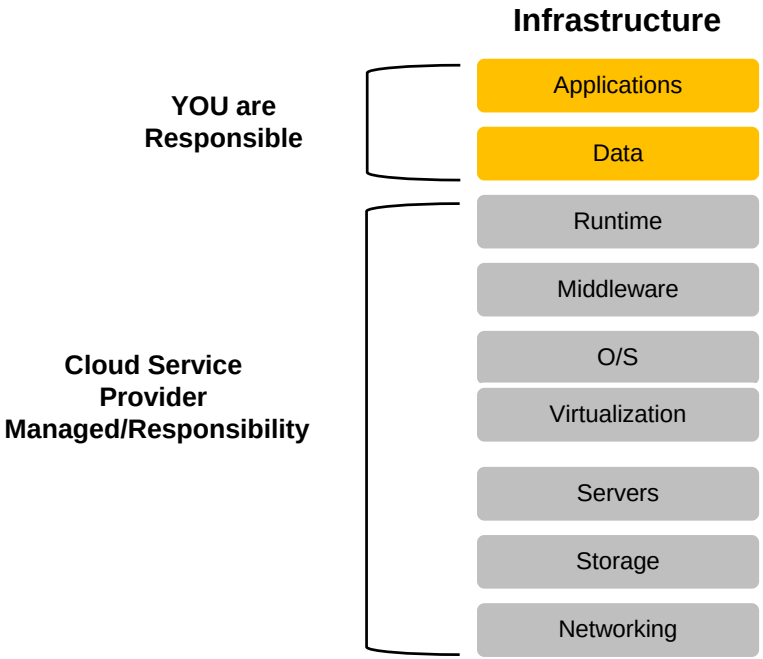
Infrastructure as a Service (IaaS)



Cloud Models (Cont.)

Vendors named within are approved or under contract to provide specified services to DISA or DOD

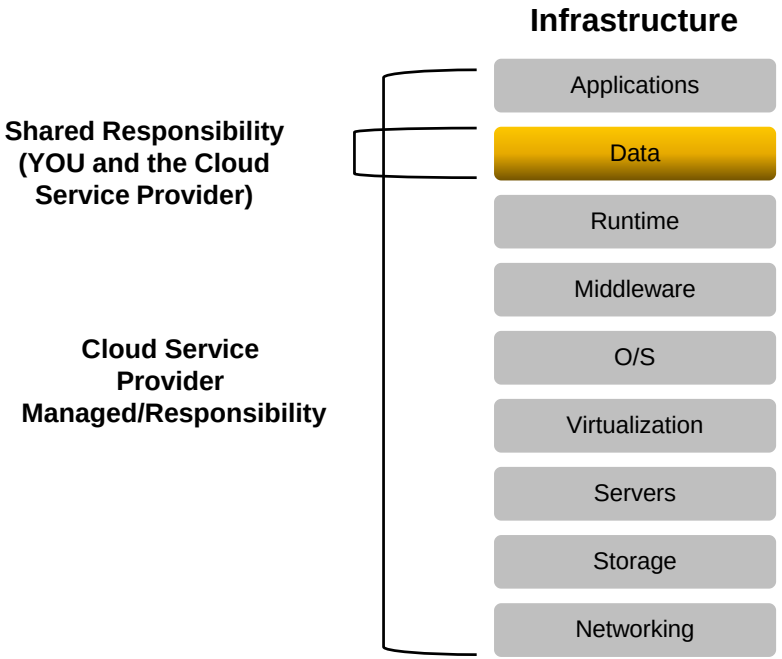
Platform as a Service (PaaS)



Cloud Models (Cont.)

Vendors named within are approved or under contract to provide specified services to DISA or DOD

Software as a Service (SaaS)



Impact Levels

Vendors named within are approved or under contract to provide specified services to DISA or DOD

- **Impact Level 2 (IL2) – Unclassified Data (public data) – requires shared or dedicated infrastructure**
- **Impact Level 4 (IL4) – Unclassified Sensitive Data (FOU, CUI, etc) – required shared or dedicated infrastructure with strong evidence of virtual separation controls and monitoring**
- **Impact Level 5 (IL5) – Unclassified Sensitive Data (NSS, PIAA, HIPA) – required dedicated infrastructure**
- **Impact Level 6 (IL6) – Classified Data (Secret, etc) – required dedicated infrastructure approved for classified information**

DEFENSE INFORMATION SYSTEMS AGENCY
The IT Combat Support Agency

Walk - Cloud Solutions

Mr. John Hale
Chief, DISA Cloud Portfolio
November, 2017

Vendors named within are approved or under contract to provide specified services to DISA or DOD

DoD Cloud Deployment Models

Vendors named within are approved or under contract to provide specified services to DISA or DOD

Best Fit Applications

On-Premise Commercial Cloud

- Commercially provided cloud service hosted within DoD facilities
- DoD security posture ensured by on premise execution
- Moderate customization to tailor the service for mission needs
- Utility pricing model “pay for usage”
- Low Total Cost of Ownership (DoD consumers share cloud cost)

- Web apps with high transactional data volume interfaces to DoDIN hosted systems or end-users on DoDIN

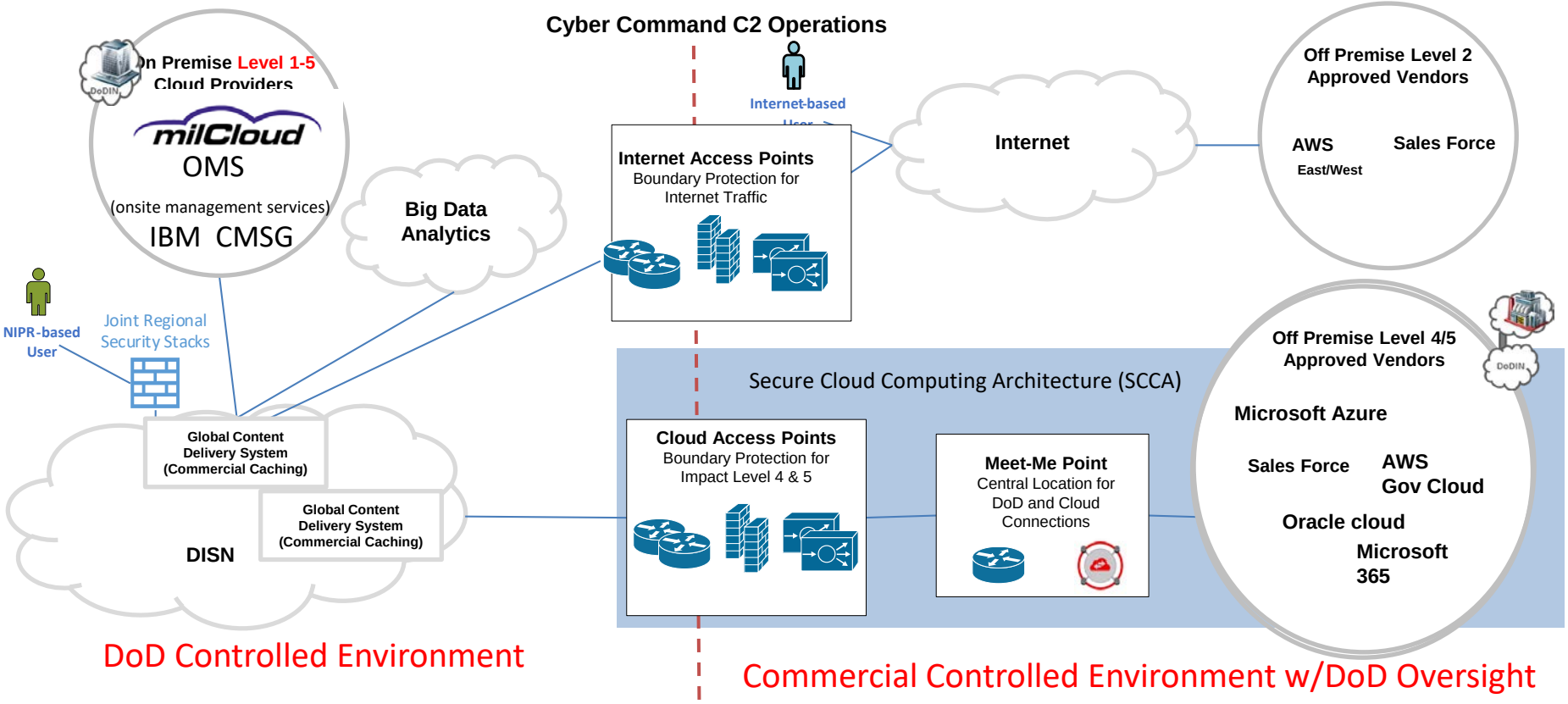
Off-Premise Commercial Cloud

- Limited customization; standard hosting across all consumers
- Broad scalability to support requirements for compute / storage
- Utility pricing model “pay for usage”
- Long Term Lowest Cost of Ownership (cloud consumers share cost of infrastructure; requires additional investment to secure)

- Level 4/5 Web apps with minimal data interfaces to “on-prem” apps
- Level 2 public information sharing Web apps with minimal data moving to DoDIN

Unclassified DoD Commercial Cloud Deployment Approach

Vendors named within are approved or under contract to provide specified services to DISA or DOD



Lessons Learned

Vendors named within are approved or under contract to provide specified services to DISA or DOD

Technical Challenges

- **Applications not cloud ready - some may never be ready due to cost to modernize**
  - **Not all app owners have access to skills and resources to modernize apps for the cloud – milCloud 2.0 and OMS include CLINs to help accelerate adoption**

- **Commercial cloud business model not always aligned to DoD heavy transactional data I/O requirements... easier for isolated applications or minimal I/O to legacy systems. (High I/O drives cost)**
  - **DoD working to provide direct network connection to small number of commercial cloud providers to offset this cost and eliminate data "meters"**

- **Applications Existing DoD Security Solutions are not cloud aware**
  - **Secure Cloud Computing Architecture (SCCA) deployed January 2018 to provide basic security services in a shared cloud environment**

Lessons Learned (Cont.)

Vendors named within are approved or under contract to provide specified services to DISA or DOD

Business Management Roadblocks

- **Business decisions challenging**
  - Lack of a single place for application owners across DoD to find all available Cloud solutions and understand which one to choose (features, price, etc.)
  - App owners don't understand new paradigm and responsibilities with commercial IaaS missing key cost in analysis (i.e. system administration, application of security, etc.)
  - Current hosting costs don't show subsidized component costs (electric, HVAC, building space, etc.) making apples to apples comparison difficult

- **Funding not available for application owners to modify apps to be cloud-ready**
  - Application rationalization data should help to decide which apps get funding for modernization

- **Policies for specific types of data (NC3, OCO) protect where data can be processed and/or stored for mission assurance**
  - App owners don’t always understand how to translate requirements to commercial facilities (search and seizure of commercial property, data sovereignty, etc.)

DEFENSE INFORMATION SYSTEMS AGENCY
The IT Combat Support Agency

Run – DISA Cloud Services

Alicia Belmas
Deputy Cloud Chief
December 12, 2017

Vendors named within are approved or under contract to provide specified services to DISA or DOD.

CLOUD COMPUTING

Vendors named within are approved or under contract to provide specified services to DISA or DOD

"The National Institute of Standards and Technology (NIST) defines cloud computing as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. The Department of Defense adopted the NIST definition of Cloud.

According to the NIST Special Publication 800-145, the Cloud model is composed of five essential characteristics, three cloud service models and four cloud deployment models

The five essential characteristics are inherent in the definition of cloud. The characteristics are:

- On-demand self service
- Broad network access
- Resource pooling
- Rapid elasticity
- Measured service

THREE CLOUD SERVICE MODELS

Vendors named within are approved or under contract to provide specified services to DISA or DOD

The three cloud service models are:

- Infrastructure as a Service (IaaS) – IaaS provides the compute, storage and networking capabilities on which a user can develop and deploy their software, which can include operating systems and software applications. The consumer is not able to manage or control the underlying cloud infrastructure.

- Platform as a Service (PaaS) PaaS is built upon the IaaS and consists of the operating systems, programming languages, libraries, services and tools. These services are supported by the cloud provider. The consumer does not manage of control the underlying cloud infrastructure nor the operating systems, but does have control over the deployed applications and possibly the configuration settings for the application-hosting environment.

- Software as a Service (SaaS) – SaaS is built upon the PaaS and provides an entire capability to a user. The consumer uses the cloud provider's applications running on the cloud infrastructure. The applications provided by the cloud provider are accessible from various client devices or platforms through either a thin client interface, such as a web browser or a program interface. The consumer does not manage or control the underlying cloud infrastructure, operating systems or even individual applications, although they may have access to limited user-specific application configuration settings.

DISA Cloud Services

Vendors named within are approved or under contract to provide specified services to DISA or DOD

Off Premise

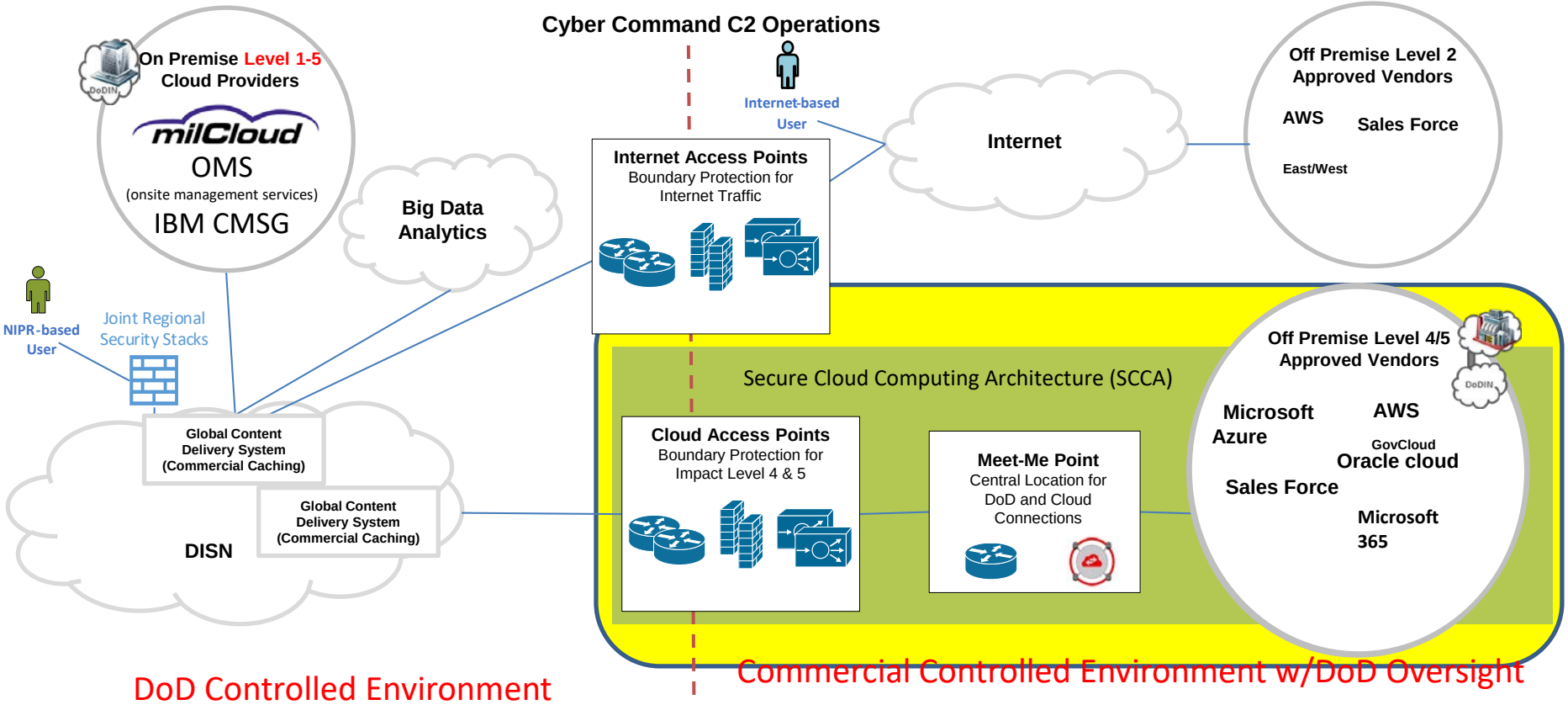
- Secure Cloud Computing Architecture (SCCA)

On Premise

- milCloud 2.0 Phase 1 (m2P1)
- On-site Managed Services (OMS)

Unclassified DoD Commercial Cloud Deployment Approach

Vendors named within are approved or under contract to provide specified services to DISA or DOD



What is SCCA?

Vendors named within are approved or under contract to provide specified services to DISA or DOD

Secure Cloud Computing Architecture (SCCA) is a suite of enterprise-level cloud security and management services. It provides a standard approach for boundary and application level security for impact level four and five data hosted in commercial cloud environments.

SCCA Suite of Services

Cloud Access Point (CAP)
- Protects DoD from cloud-originated attacks
- Connectivity for IaaS and SaaS

Virtual Data Center Security Stack (VDSS)
- Traditional DMZ security for public facing applications
- Next generation firewall to protect cloud hosted workloads

Virtual Data Center Managed Services (VDMS)
- Cloud connected management and security tools
- Privileged user access and management

Trusted Cloud Credential Manager (TCCM)
- Role based access control and least privileged success

SUITE OF SERVICES OVERVIEW

Vendors named within are approved or under contract to provide specified services to DISA or DOD

BOUNDARY CAP Key Features

- NIPRnet connectivity support for IaaS and SaaS clouds
- Security tools focused on protecting the DISN from the cloud
- Operational and security intelligence data via logging and Netflow

VDSS Key Features

- Traditional DMZ security features for public facing web applications
- Next Generation Firewall for protecting cloud hosted workloads

VDMS Key Features

- Cloud connected management and security tools
- Cloud privileged user access and account management
- Central search and display of CAP and Cloud logs via Splunk

TCCM Key Features

- Privileged password management and control
- SSH Key security and management
- Session manager to control and monitor privileged user access to IaaS clouds and hosted instances
- Bastion host for access into all management and security services

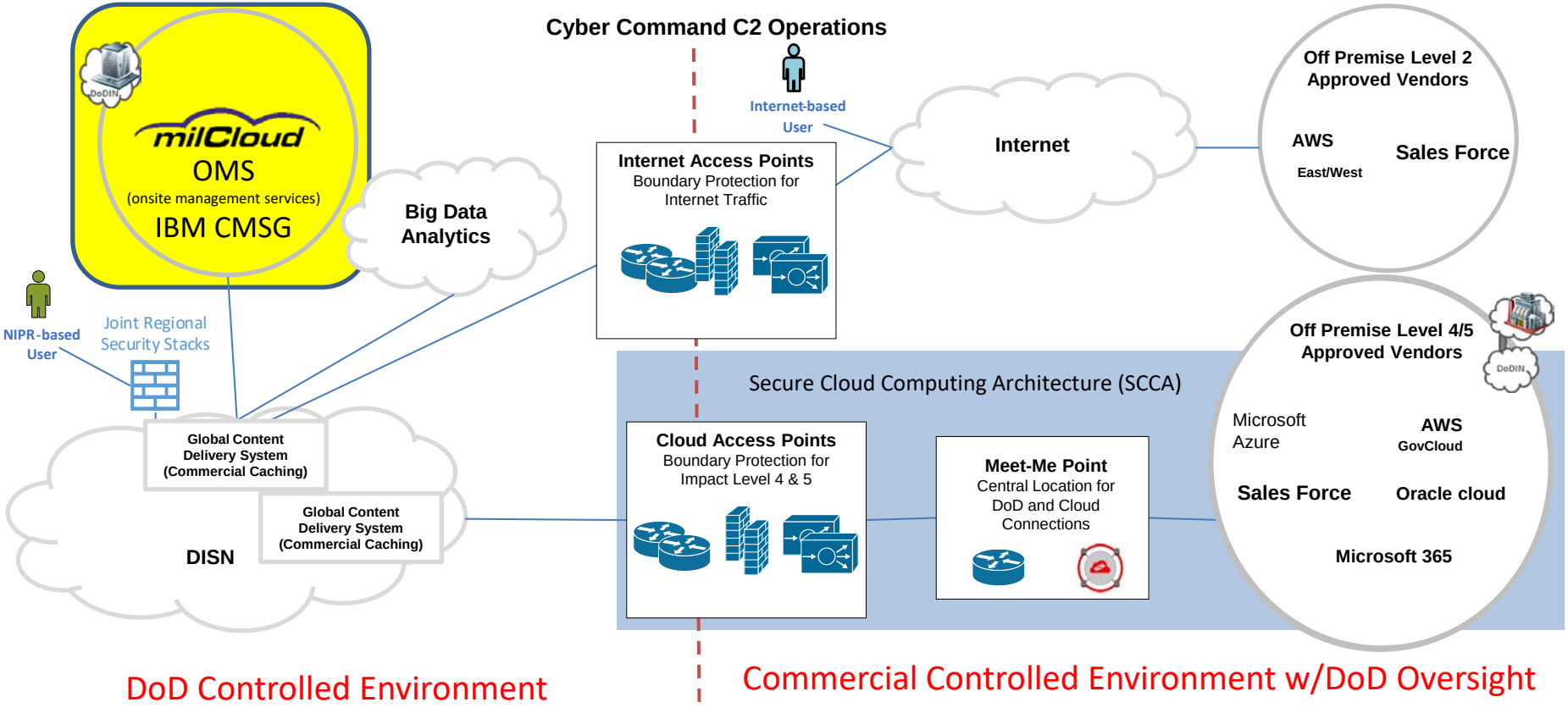
VDMS Service Offerings

Vendors named within are approved or under contract to provide specified services to DISA or DOD

Service	Description	Capabilities
HBSS	Cloud integrated ePolicy Orchestrator (ePO) management and SuperAgent Distributed Repository (SADR)	• Install host agents • Configure and deliver security policies • Download and push upgrades • View data and generate reports
ACAS	Cloud integrated Tenable Security Center and Nessus vulnerability scanners	• Manage roles • Create scan zones and policies • Schedule and run compliance scans • Manage server credentials
Operating System Patching	Cloud based versions of DoD patch repositories	• Integrated with on-premise DoD repositories
Recursive DNS Caching	Recursive DNS server in the extension to forward and cache external DNS queries	• Cashes responses to provide DNS response times for lookups • Eliminates requirement for cloud mission owner to connect from cloud environment enclave to ERS
Cloud Visibility	Logs and Netflow data will feed enterprise Splunk for visibility and support security incident and event management (SIEM)	• Centralized through the VDMS core • Future multi-tenant options will enable tailored search and display for multiple CSSP providers

Unclassified DoD Commercial Cloud Deployment Approach

Vendors named within are approved or under contract to provide specified services to DISA or DOD



What is m2P1?

Vendors named within are approved or under contract to provide specified services to DISA or DOD

m2P1 is a commercially-owned commercially-operated on-premises private cloud. That establishes a commercial Infrastructure as a Service (IaaS) environment in DISA Data Centers that are connected to DoD networks and have unclassified workloads transitioned to and stored in the commercial IaaS solution. It is a "pay for usage" model instead of charging for capacity by the month. m2P1 will offer Red Hat Open Shift as it's PaaS offering.

- **milCloud 2.0 portfolio common cloud services characteristics:**
  - On-Demand, Self-service: milCloud consumers can place orders on-demand through web-based self-service tools, configure infrastructure resources where appropriate, and manage their mission application's lifecycle running on those resources without manual intervention from DISA or CSP support staff
  - Broad Network Access: All milCloud products and services have network connectivity to the Department of Defense Information Networks (DoDIN), and are configured in accordance with relevant DoD security guidelines and approved protocols
  - Resource Pooling: milCloud resources are pooled such that multiple mission partners consume units from pools provisioned by DISA, enabling efficient use of aggregate compute resources and greater consumption flexibility
  - Rapid Elasticity: milCloud has the ability to expand or contract their resource use within virtual resource pools

m2P1 Services

Vendors named within are approved or under contract to provide specified services to DISA or DOD

m2P1 key contract features – Awarded June 9, 2017

- Single award IDIQ (full and open)
- POP (3) year base with (5) one year options
- Life cycle value $498M
- DoD Data Center's Montgomery (Prime) & Oklahoma City (Secondary) are the two site locations

m2P1 key services through the web portal

Metered Billing

- Only pay when it is in a billable state

Finer billing units

- Servers – by the hour
- Storage – by the GB per day

Monitoring and alerting through the m2P1 cloud web portal

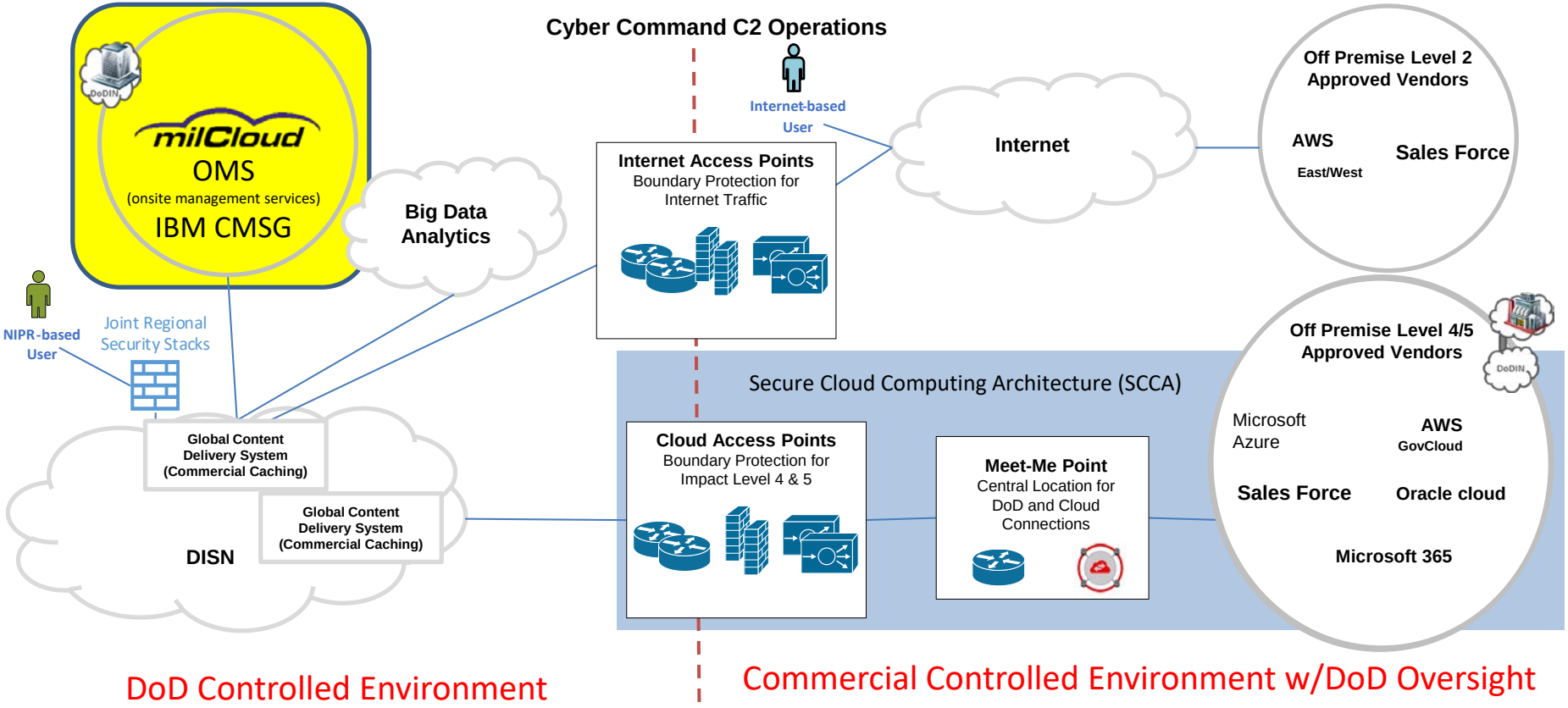
- Always know how much you are spending, and how much you have left

Flexible funds utilization – Purchase Cloud "Units"

- Provide Funds based on your initial estimate
- Configure and reconfigure as needed – Servers, Storage, Core Services

Unclassified DoD Commercial Cloud Deployment Approach

Vendors named within are approved or under contract to provide specified services to DISA or DOD



What is OMS?

Vendors named within are approved or under contract to provide specified services to DISA or DOD

OMS is commercially-owned commercially-operated Infrastructure as a Service (IaaS) and Platform as a Service (PaaS). OMS is built on VMware that supports PaaS based on the Pivotal Cloud Foundry (PCF). OMS is designed to minimize system and application changes required to migrate applications to the cloud.

OMS common cloud services characteristics:

- On-Demand, Self-service: OMS consumers can place orders on-demand through web-based self-service tools, configure infrastructure resources where appropriate, and manage their mission application's lifecycle running on those resources without manual intervention from DISA or CSP support staff
- Broad Network Access: All OMS products and services have network connectivity to the Department of Defense Information Networks (DoDIN), and are configured in accordance with relevant DoD security guidelines and approved protocols
- Resource Pooling: OMS resources are pooled such that multiple mission partners consume units from pools provisioned by DISA, enabling efficient use of aggregate compute resources and greater consumption flexibility
- Rapid Elasticity: OMS has the ability to expand or contract their resource use within virtual resource pools

OMS Services

Vendors named within are approved or under contract to provide specified services to DISA or DOD

OMS key contract features – Awarded September 2016

- Single award IDIQ (full and open)
- POP (1) year base with (4) one year options
- Life cycle value $98M
- DoD Data Center's Ogden, UT site location

OMS On boarding features

- Staffing & Onboarding
  - Provide staff access & resources
  - Train staff and perform Delivery Assurance Assessment
- Process Integration
  - Integrate mission policies and processes with best practices delivery model
  - Implement best practices, process readiness, measurements, and controls to meet service performance standards
- Service & Technology Reporting
  - Implement reporting measurements for service & technology management controls
  - Publish service and technology reports demonstrating service delivery meets performance standards
- Technology Management Integration
  - Implement technology management infrastructure, operational readiness, measurements and controls to meet service performance standards

DEFENSE INFORMATION SYSTEMS AGENCY
The IT Combat Support Agency

Fly – DISA Cloud Adoption Playbook

Alicia Belmas
Deputy Cloud Chief
December 12, 2017

Vendors named within are approved or under contract to provide specified services to DISA or DOD

DEFENSE INFORMATION SYSTEMS AGENCY
The IT Combat Support Agency

UNITED IN SERVICE TO OUR NATION

Vendors named within are approved or under contract to provide specified services to DISA or DOD