



DEPARTMENT OF THE NAVY CHIEF INFORMATION OFFICER

DON Cloud Update

Susan Shuryn

DON CIO Cloud Computing Lead

21 April 2016

Agenda

- **What Have We Learned**
- **Recent DON Policy**
- **Current DON Efforts**
- **Governance**
- **Data Owner Considerations**
- **Hosting Onboarding**
- **Managed Service Models**
- **Commercial Cloud Transition Progress**
- **DISA / DoD Next Steps**
- **Panel Discussion – Moving from Pilot to Production**

What Have We Learned?

- **Educate**: yourselves and others about Cloud Computing in DoD
- **Train**: invest in training operational support manpower
- **Understand**: roles for providers, integrators, government
- **Read**: follow policy and regulations; stay current
- **Determine**: data ownership responsibilities/requirements
- **Develop**: designs with cybersecurity requirements in mind
- **Authorize**: Involve your AO Office early in the development

Recent DON Policy

Updated DON Guidance on the Acquisition and Use of Commercial Cloud Computing Services: DON CIO Memo- April 2016

- **Analyze first** - use Business Case Analysis (BCA) template (available on DON CIO website: <http://www.doncio.navy.mil/>, include DISA milCloud in the estimate)
- **Submit BCA** - and Engineering Assessment (EA) to your DDCIO for approval via the current IT procurement approval process
- **Understand contracting rules**- the latest DON policy references DFARS clause for cloud computing contracts
- **Contact the Navy Managed Service Organization (MSO)** - PEO EIS / Data Center and Application Optimization (DCAO) Team: spawar-dcao-esm.FCM@navy.mil
- **Know your system requirements** - Federal Risk Authorization and Management Program (FedRAMP) or FedRAMP + is required for confidentiality; availability requirements must be in your contract

Current DON Efforts

- **Navy Cloud Store 1.0 Opens March 2016**
 - Received Navy Authority To Operate (ATO) for Level 4-5 data
 - Data traverses the DoD Authorized Navy Cloud Access Point (CAP)
 - East Coast CAP complete; West Coast circuit/meet me point being built
 - Level 4 applications preparing for ATO and migration
 - Participants in DoD Commercial Cloud pilots; tracked by DoD CIO
- **Implemented DON Policy and Processes**
 - Incorporated BCA and EA into IT Procurement Request Process
 - Continue evolving Governance as more Providers become authorized
 - Developing operational service model processes for commercial cloud
- **Continuing Various R&D Work with Authorized CSPs**
 - Various Private/Hybrid Cloud environments
 - Public /Community Cloud Portals
 - Incorporate experience/lessons learned into operational process

Cloud Governance

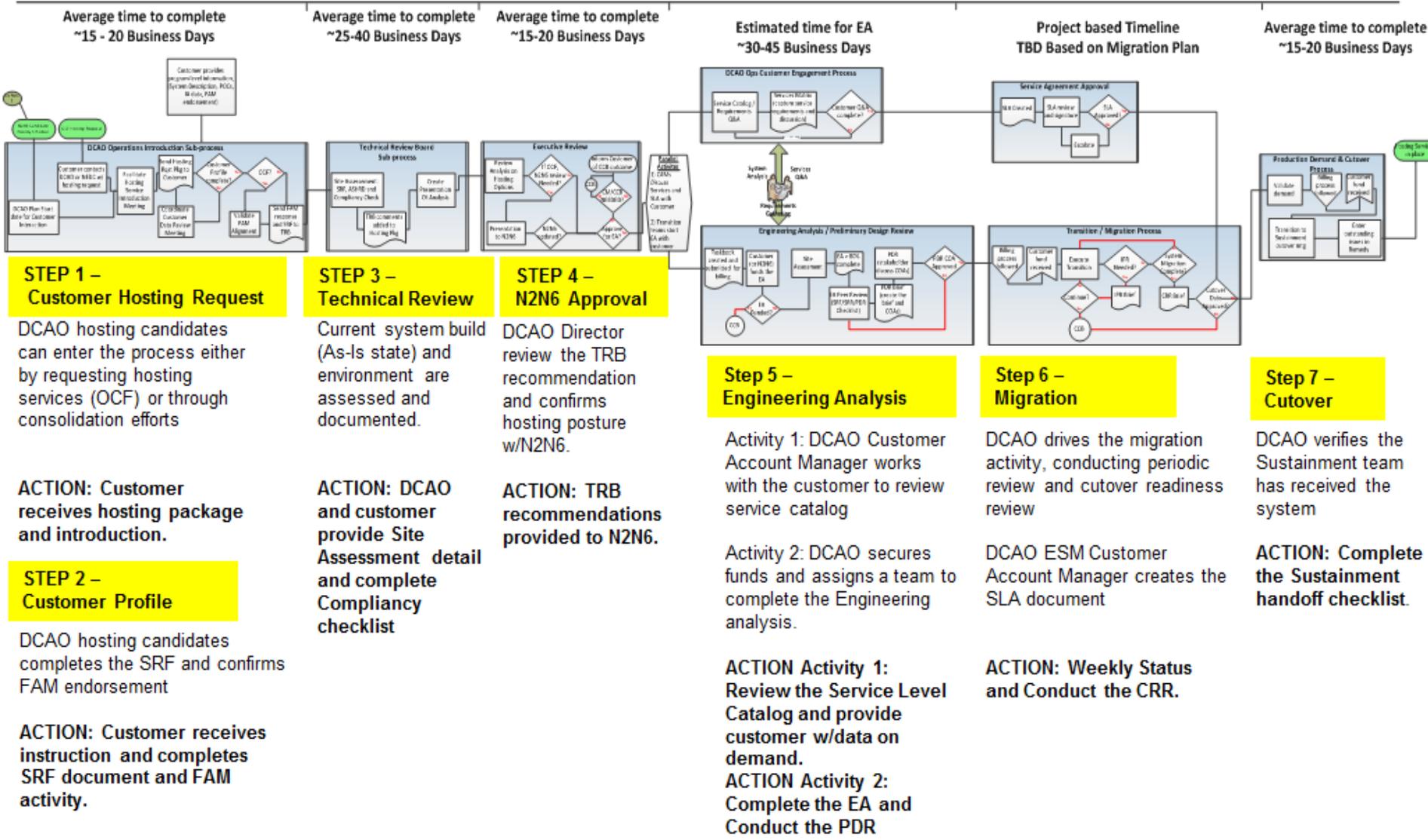
- **Background.** The Navy intends to be “Cloud First” with a goal to move 75% of Navy IT capabilities (systems, applications, and services) to the commercial “cloud” by 2022.
- **Governance is centralized.** It is designed to be measurable, repeatable, and consistent. DCAO is tasked as the Cloud Broker and is responsible for contracts and tech standards.
- **Current Process – includes these main steps:**
 - Contact DCAO: spawar.dcao.esm.FCM@navy.mil
 - Tech Review or Engineering Assessment (EA)
 - BCA development, assessed against milCloud and or NEDCs
 - Cloud request with BCA submitted via NAVIDAS for approval
- **Note:** Capabilities in a commercial cloud are not considered in a “data center.”

Data Owner Considerations

- **Determine Information Security Impact Level**
 - Must traverse CAP for level 4 and above
- **Determine appropriate Service Model**
 - IaaS, PaaS, SaaS
- **Review CSP physical locations / Characteristics / Authorizations**
 - Determine appropriate deployment model
- **Align with CSP Personnel Investigation Requirements**
 - Appropriate investigations based on OPM and DoD requirements
- **Consider Infrastructure sharing with other systems**
 - Trust between systems, e.g., AD trust relationships, Sys Admin, Coop/DR
- **Contract Considerations (SLAs, data return/wipe, incident response)**
 - Availability requirements must be determined and included in the contract/SLA

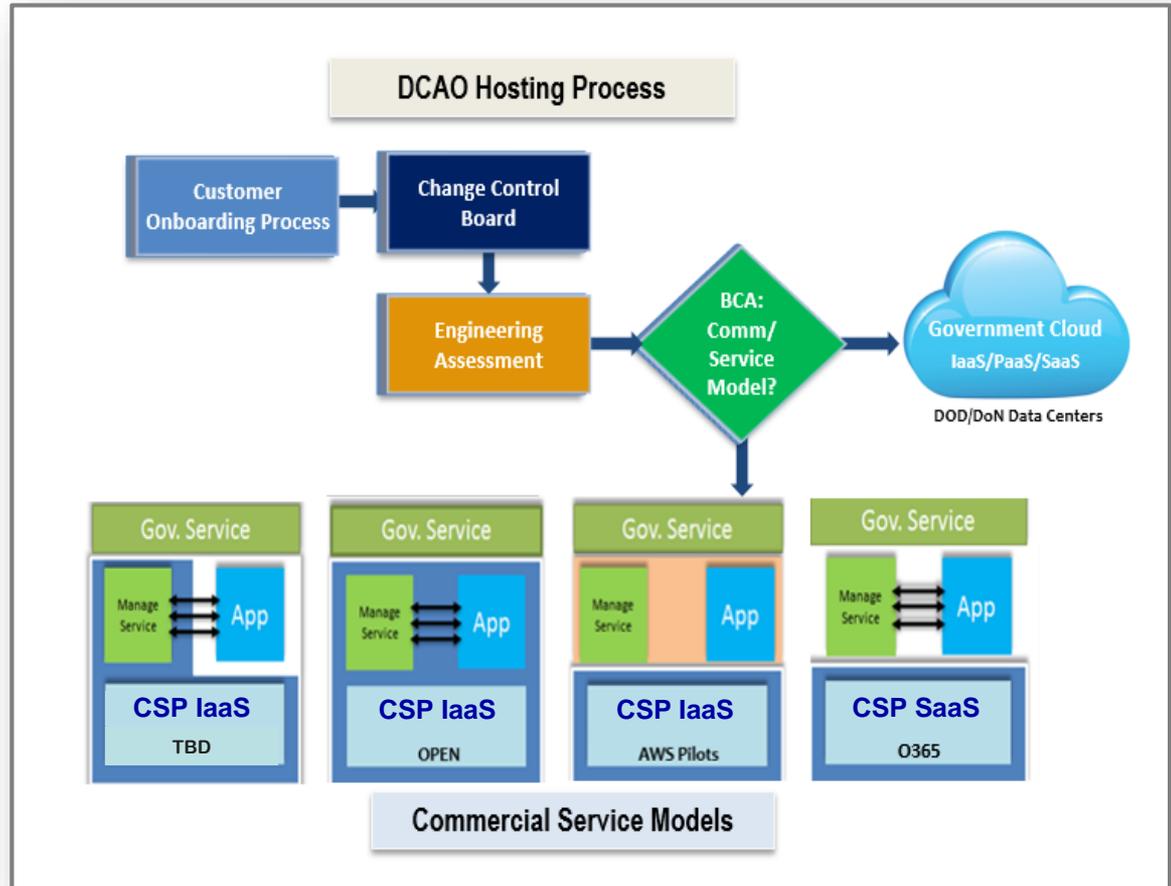
Common Hosting Onboarding Model (same for commercial cloud)

Hosting Process Steps - Notional Timeline: shown by step



Managed Service Models

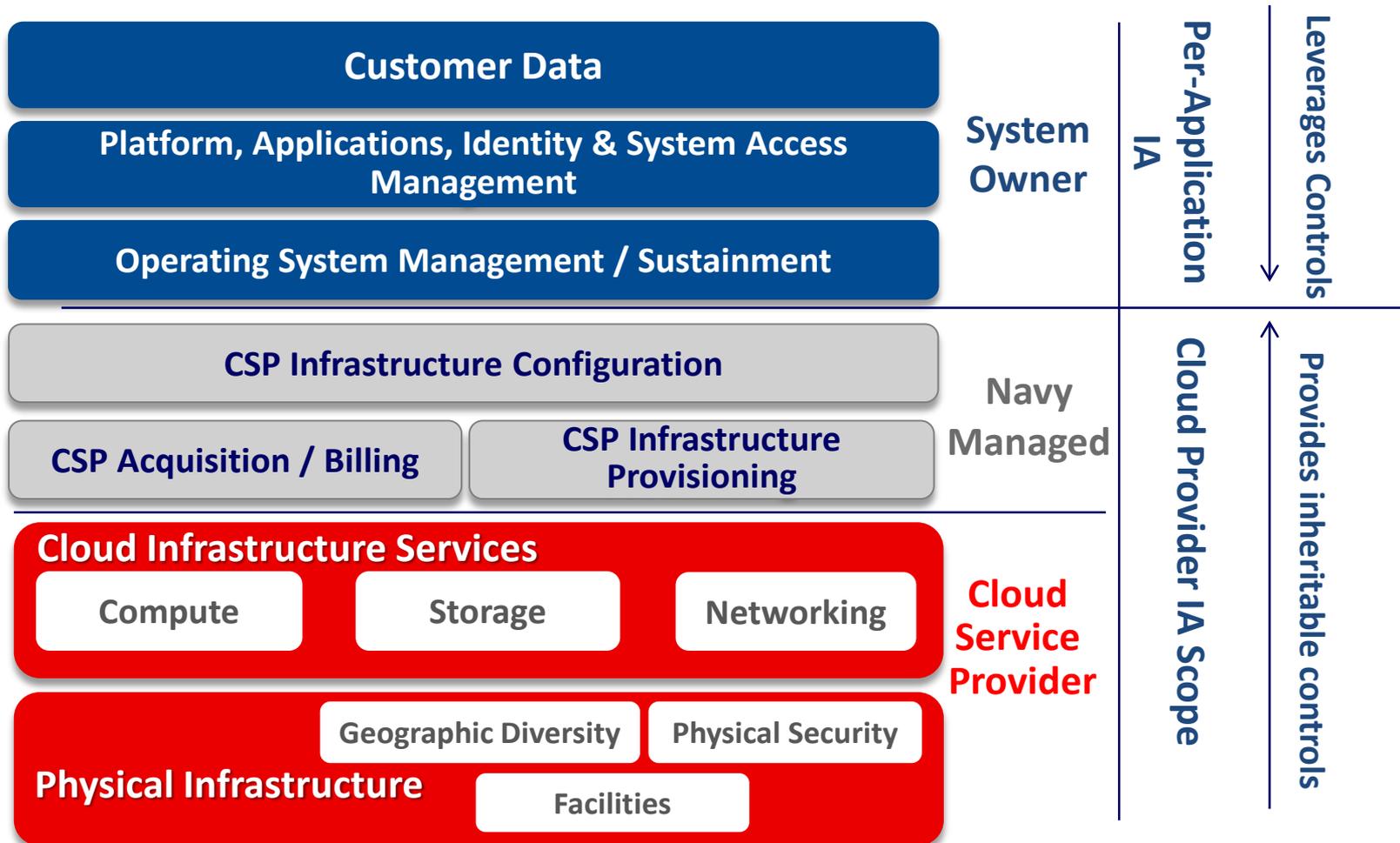
- DCAO is developing a phased approach to Commercial Service Model implementation
 - Governance required for sustainable and repeatable processes
- Commercial Hosting Lessons Learned to date:
 - Establish Cloud Service Strategy; learn small (low risk)/evolve big
 - Leverage existing DCAO process model
 - Integrate cloud-specific activities into DCAO hosting process and service design model (Service Catalog, Rate Card, SLAs)



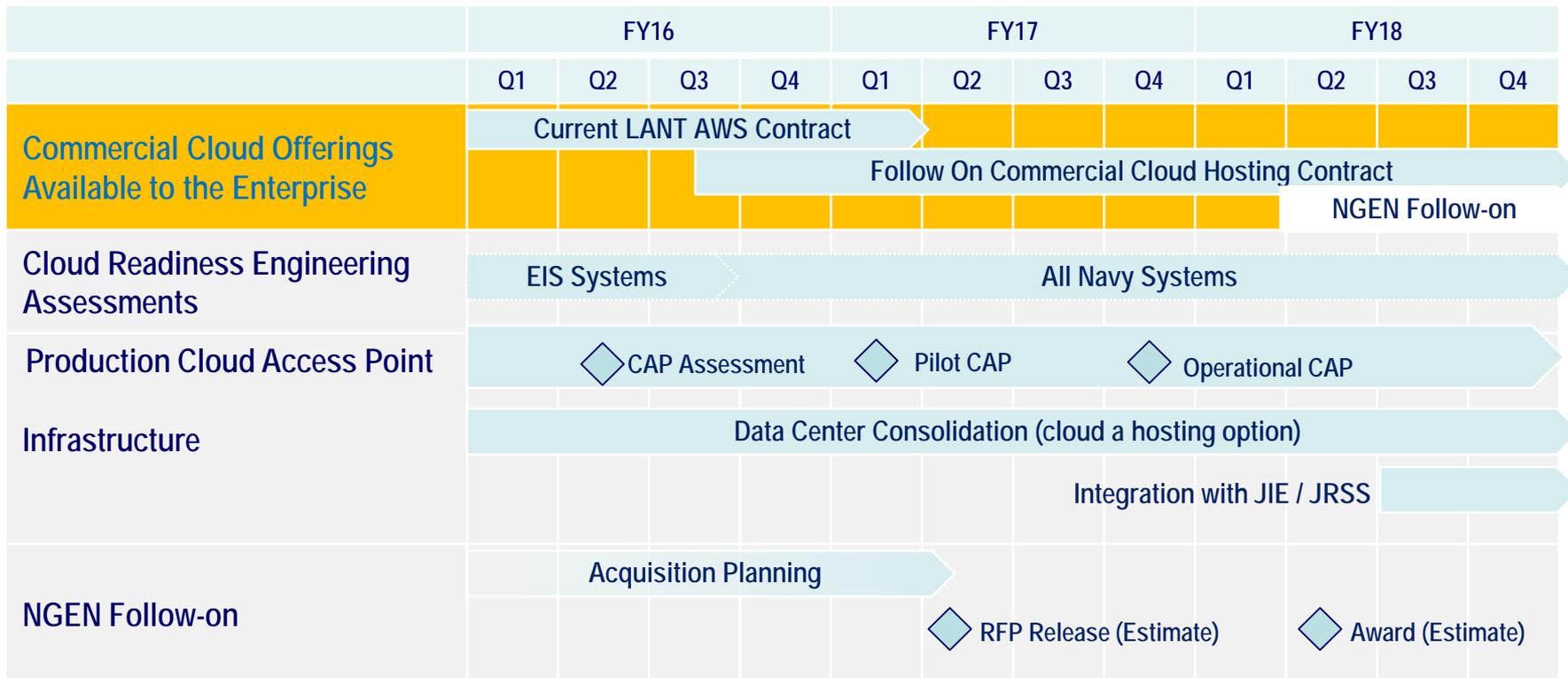
Commercial Hosting Supports Data Center Consolidation (DCC) Objectives

Navy Cloud Managed Service Model (IaaS)

Managed Services in a Shared Responsibility / Inheritance Model



Commercial Cloud Transition Progress



Learning from pilots, and incrementally increasing cloud capability for the Navy

FedRAMP / DoD Certification Cloud Security Requirements Guide (CSRG)

Data Impact Level	FedRAMP	DISA Authorization	Navy 8500 ATO	CAP Usage	Physical Isolation
CSRG L2	✓	★★	✓		
CSRG L4	✓	✓	✓	✓	
CSRG L5	✓	✓	✓	✓	✓
CSRG L6	✓★	✓	✓	✓	✓

★ Pending release of FedRAMP High controls

★★ Required by FAR update, DISA grants L2 PA to all FedRAMP approved CSPs

- ▶ Navy Information Systems are still required to meet all DoD Instructions (e.g., 8500), Joint Chiefs Instructions (e.g., 6510) and USCC CTOs (e.g., 07-12/HBSS)
 - Migrating to the cloud does not eliminate any standing policy requirement
- ▶ The FedRAMP and DISA evaluations are intended to be used in a reciprocity-based fashion by the Navy Authorizing Official
 - Navy does not have to perform IV&V and audit of the cloud providers infrastructure – the assessment can be re-used saving significant time/labor/funding
- ▶ DISA will collaborate with the Services to allow Services IV&V and audit results of a CSP to inform a DISA Authorization

Cloud Service Providers: Level 4-5 DoD Provisional Authorizations

Either Complete or In Process of Obtaining DoD Provisional Authority

CSP Offering	Type	Lvl	Scope	Phase	3PAO	Assessor	DoD PA Issued
Amazon AWS GovCloud (Conditional PA for Pilots)	IaaS	4	FedRAMP+DoD	Extension	Veris	DISA	01 Feb 2016 (2 month Extension)
Oracle Service Cloud (DoD OSC)	SaaS	4	FedRAMP+DoD	Complete	N/A	DISA	14 Aug 2015 (2 yr)
IBM CMS-G	IaaS	5	FedRAMP+DoD	SSP/SAP/SAR	Veris	DISA/Army	05 Feb 2016 (First Use limited to NAVSEA / DLA)
Microsoft O365 DITAR	SaaS	5	FedRAMP+DoD	SSP/SAP/SAR	Kratos	DISA/SPAWAR	Est for Conditional May - June 2016
Microsoft O365 ITAR	SaaS	5	FedRAMP+DoD	SSP/SAP/SAR	Kratos	DISA/AF/DLA	Est Aug - Sept 2016
Box	SaaS	4	FedRAMP+DoD	SSP/SAP/SAR	Brightline	DISA/AF	TBD

Current DISA/DoD Efforts

- **Cloud Connection Process Guide collaborative work in process**
- **Cloud Security Requirements Guide V1R2 published in March**
- **Integrating CSP Cloud Service Offering information into tools such as eMASS to support RMF package inheritance**
- **Conducted Joint DoD/Industry CND TTX in December 2015**
- **DODI 8530.01 "Cybersecurity Activities Support to DoD Information Network Operations" was released in March**
- **Draft Secure Cloud Computing Architecture Functional Requirements (CAP 2.0) published in March**
- **Contracting language - DFARS clause in review process**

Panel Discussion

Cloud Computing in the DON Lessons Learned

Commercial Cloud Transition Progress

Opening the Store



Service Offering

- Managed Service Organization
- ✓ L2/4 IaaS Hosting
- ✓ Limited Shared Services
- ✓ Aligned to DCAO Hosting Process

Customers

PEO EIS
 ENTERPRISE INFORMATION SYSTEMS
 DEPARTMENT OF THE NAVY

Cloud Pilot List- Level 4/5

Application	Hosting Steps						
	1	2	3	4	5	6	7
DoD Pilot Applications							
NIPO Facts	✓	✓	✓	✓	✓	✓	Apr-16
PRISM	✓	✓	✓	✓	✓	✓	Jun-16
DEKES	✓	✓	✓	✓	✓	✓	Mar-16
Pilot Applications							
CAMEO RIC Implementation	✓	✓	✓	✓	✓	✓	Dec-16
My Navy Portal	✓	✓	✓	✓	✓	✓	Oct-16
NITES Next Implementation	✓	✓	✓	✓	✓	✓	Oct-16
NHHC-KE	✓	✓	✓	✓	✓	✓	
ONI/NRL MORSD	✓	✓	✓	✓	✓	✓	
NAVSEA SUPSAU	✓	✓	✓	✓	✓	✓	
NAVRES Office 365 Support	✓	✓	✓	✓	✓	✓	
DCC Baseline Candidate- Impact Level 4							
SMART-T	✓	✓	✓	✓	✓	✓	
MELS	✓	✓	✓	✓	✓	✓	
NIPDP	✓	✓	✓	✓	✓	✓	
Navy Shook Database (NSD)	✓	✓	✓	✓	✓	✓	
Boats Inventory Management (BIMS)	✓	✓	✓	✓	✓	✓	
Inactive Ships Management (ISMS)	✓	✓	✓	✓	✓	✓	



Service Offering

- ✓ Cloud Management Services
- ✓ Multiple L2/4/5 IaaS CSPs
- ✓ Robust Shared Services
- ✓ Thin Government Management Layer
- ✓ Aligned to DCAO Hosting Process

Customers

PEO EIS
 ENTERPRISE INFORMATION SYSTEMS
 DEPARTMENT OF THE NAVY

OCF Hosting Requests

DCC Baseline Candidates Impact Level 4

Application	Phase	Customer
SMART-T	Step 4	VADM RI
MELS	Step 4	NSWC SHIPSYENGSTA
NIPDP	Step 4	NSWC SHIPSYENGSTA
Navy Shook Database (NSD)	Step 4	NSWC SHIPSYENGSTA
Boats Inventory Management (BIMS)	Step 4	NAVSEA - NSVIC Cranbrook
Inactive Ships Management (ISMS)	Step 4	NAVSEA - NSV Portsmouth

FY17 Deferred List adds more...

- ✓ Level 2 Hosting is happening now (OPEN, DONAA, MARCIMS)
- ☐ Navy Cloud Store 1.0 opens ~March 2016
- ☐ Navy Cloud Store 2.0 opens ~ Q1FY17

Back Up

NIST Definition of Cloud Computing

- 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)
- Can be rapidly built and released with minimal management effort or service provider interaction
- Composed of five essential characteristics, three service models, and four deployment models:

Essential Characteristics:

1. *On-demand self-service*
2. *Broad network access*
3. *Resource pooling*
4. *Rapid elasticity*
5. *Measured service*

Service Models:

1. *Software as a Service (SaaS)*
2. *Platform as a Service (PaaS)*
3. *Infrastructure as a Service (IaaS)*

Deployment Models:

1. *Public cloud*
2. *Community cloud*
3. *Private cloud*
4. *Hybrid cloud*

Deployment Model Definitions

- **Public cloud:** Infrastructure is provisioned for open use by the general public; exists on the premises of the cloud provider
- **Private cloud:** Infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers; may exist on or off provider premises
- **Community cloud:** Infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns; may exist on or off provider premises
- **Hybrid cloud:** Infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but bound by standardized or proprietary technology; location depends on specific model

Information Impact Levels

Definition: Impact Levels are defined by a combination of 1) level of data to be stored/processed and 2) potential impact of an event resulting in the loss of confidentiality, integrity or availability of data, systems, or networks. The security control baseline for all Impact Levels is based on moderate confidentiality and moderate integrity (FIPS - 199). Categorize systems IAW DoDI 8510.01 and CNSSI 1253. Availability is determined by mission owner and should be specified in the contract.

SRG v1r1 Impact Level	Maximum Data Type	Information Characterization
2	Non-Controlled Unclassified Information	Unclassified information approved for public release
		Unclassified, not designated as controlled unclassified information (CUI) or critical mission data, but requires some minimal level of access control
4	Controlled Unclassified Information	Requires protection from unauthorized disclosure as established by Executive Order 13556 (Nov 2010); Education, Training, SSN, Recruiting (if medical is not included), Credit card information for individuals (i.e., PX or MWR events)
		PII, PHI, SSN, Credit card information for individuals, Export Control, FOUO, Law Enforcement Sensitive, Email??
5	Controlled Unclassified Information + NSS	National Security Systems and other information requiring a higher level of protection as deemed necessary by the information owner, public law, or other government regulations
6	Classified up to/including SECRET	Pursuant to EO 12958 as amended by EO 13292; classified national security information or pursuant to the Atomic Energy Act of 1954, as amended to be Restricted Data (RD)