Enabling NASA Software-as-a-Service (SaaS) Use

Computing Services Program Office
Enterprise Managed Cloud Computing (EMCC) Service Office

Version 1.0, September 29, 2016
The NASA Enterprise Managed Cloud Computing (EMCC) Service Office facilitates secure and policy compliant Agency access to commercial cloud services (IaaS, PaaS, and SaaS).

Addresses services, standards, guidance, governance approach, and technical integration to greatly reduce the burden associated with gaining approved NASA access to the rich and rapidly growing marketplace of cloud-based applications and services.

An enterprise approach results in faster adoption, greater consistency, managed risks, and lower Agency costs.
If each NASA community or project addresses the wide array of Requirements for Cloud Computing:

- Projects may interpret and fulfill requirements differently
- Unknown security posture and risks
- Inconsistencies in policies, processes, and implementations
- Highly inefficient approach that results in large Agency spend
- Chaos

Do the “heavy lifting” once for the Agency and enable projects to leverage the capabilities we’ve created.

Goal: All cloud use at NASA shall be MANAGED cloud use
NASA OCIO Computing Program Goals For SaaS

Goals are aligned with Federal, Agency, and OCIO guidance, mandates, goals, and objectives.

<table>
<thead>
<tr>
<th>Long-Term End Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. NASA experiences widespread adoption of cloud computing by programs and projects.</td>
</tr>
<tr>
<td>2. NASA uses Commercial SaaS to address program and project requirements when it is the best available approach.</td>
</tr>
<tr>
<td>3. NASA-used SaaS is governed, managed, and operated using an enterprise-managed approach.</td>
</tr>
<tr>
<td>4. NASA SaaS management processes are open and malleable to enable service innovation.</td>
</tr>
</tbody>
</table>
EMCC Application Portfolio Focus

ALL Applications In use at NASA

All APPROVED Apps In use at NASA

All Commercial Cloud Apps In use at NASA (SaaS)

NASA developed or commercial, cloud or non-cloud

EMCC Focus
Computing Services Strategy

- Reduces use of unsanctioned services
- Improves Agency risk posture
- Brings IT services under enterprise management
- Provides a unified services delivery approach
- Enables innovation to address mission requirements
Why a Platform is Needed

- Explosive growth in SaaS usage cannot be managed using manual approaches
- Provides a unified approach to delivering IT services (Cloud and Data Center), thereby improving the user experience
- Increases efficiency and productivity via workflow automation (e.g., auto-provisioning, license management)
- Consolidates pockets of service usage, enabling Agency buys with discounts
- Leverages reseller service bundles, accelerating development of services portfolio
- Provides existing Agency data centers with a platform to reach new customers

Services delivery platform solutions (e.g., cloud brokering platforms) are emerging to address cloud computing and hybrid IT.
SaaS High-Level Business Strategy

Key Elements of SaaS Strategy

1. Deploy an Agency-wide SaaS storefront (marketplace) where customers can easily and quickly purchase and use SaaS apps.
2. Develop and empower network of internal service providers at Centers to evaluate, onboard, and curate SaaS apps for Agency-wide use.
3. Where possible, acquire bundles of SaaS services from cloud brokers to reduce cost of managing individual services.
4. Give precedence in the early stages to SaaS apps that can be onboarded to the Minimal Risk Portfolio (MRP).

The CSPO extends its Cloud Services Delivery Network to Centers to leverage resources to address the significant demand for SaaS.
The Wholesale and Retail Platforms provide core capabilities that extend across all markets (Agency, Centers, Projects) to unify the delivery of services across the Cloud Services Network.
**SaaS Enterprise Implementation Strategy**

Driving Objectives: Gain visibility into the SaaS products already in use, assess risk due to the low level of governance that has been applied to those SaaS products in the past, and make the transition to Agency-level managed SaaS.

### Deploy Security Framework
- A&A processes and guidance
- Cloud Access Security Broker tool (CASB)
- Establish technical integrations including authentication, networking, security operations

**Enables centers to onboard new SaaS in a safe and compliant way**

### Audit and Cleanup Existing SaaS
- Triage the list to prioritize biggest risks
- Audit usage
- Establish any special rules or constraints
- Establish center ownership and who will perform assessment

**Brings existing SaaS into compliance and reduces Agency risk**

### Develop SaaS Business Environment
- Identify SaaS vendor business models
- Define ownership and curation requirements
- Determine best procurement approach
- Define ordering and payment and renewal mechanism

**Enables enterprise management of SaaS business aspects**
SaaS CONOPS Framework

1. Identification
   1.1 Service Inquiry Management
   1.2 Service Usage Discovery

2. Authorization
   2.1 Service Characterization
   2.2 Sanctioning Proposal Development
   2.3 Service Sanctioning

3. Onboarding
   3.1 Procurement
   3.2 Service Offering Definition
   3.3 Business and Technical Integrations
   3.4 Service Incorporation Within MCE
   3.5 Service Launch

4. Operations
   4.1 Service Management
      4.1.1 Service Lifecycle Management
      4.1.2 Service Request Management
      4.1.3 Budgeting/Cost Estimation
      4.1.4 Request Approvals
      4.1.5 Spend Management
      4.1.6 Access Management
   4.2 Administration
      4.2.1 Billing Account Management
      4.2.2 Account Funding/Replenishment
      4.2.3 Licensing
      4.2.4 Renewals
      4.2.5 Statement/Invoice Generation
      4.2.6 Payments (vendors)
      4.2.7 Financial Reporting
   4.3 Service Asset Mgmt
      4.3.1 Service Instance Provisioning
      4.3.2 Capacity Management
      4.3.3 Performance Management
      4.3.4 Service Incident Management
      4.3.5 Security Monitoring
      4.3.6 Security Incident Management
      4.3.7 Data Integrity/Backup

5. Offboarding
   5.1 Service Retirement Decision/Planning
   5.2 Data Archive/Migration
   5.3 Service Instances Retirement
   5.4 Service Retirement
Cloud Access Security Brokers (CASB) are on-premise or cloud-hosted software that act as a control point to secure cloud services. Range of capabilities may include:

- **Visibility**: Dashboards, identification of approved vs unapproved applications, analytics, incident reporting, policy control, automated alerting and reporting, license counts and usage, identification of “shadow IT”
- **Compliance**: Role based auditing, file content monitoring for compliance to PII, HIPAA, etc., policy enforcement
- **Data Security**: DLP, Encryption, Tokenization
- **Threat Protection**: inbound/outbound content monitoring, user behavior analytics, prevent prohibited devices and locations from accessing network, anomaly detection
- **Enterprise Integration**: ICAM, centralized log management, secure web gateway/proxies

**By 2016, 25% of enterprises will secure access to cloud-based services using a CASB platform, up from less than 1% in 2012, reducing the cost of securing access by 30%**.

• Per Gartner, most of today's SaaS aggregation platforms support commercial service providers looking to broker SaaS services via a marketplace or app store to **external customers**.

• A few providers are expanding their offer to also support **internal IT** departments.

• EMCC is monitoring developments and new offerings in this space closely, as this such a capability is a key component of the SaaS business strategy.
Key Enabling Construct: Agency Cloud Service Portfolios

CSP On-Boarding Request

Agency General Purpose Portfolio

Agency Services

Agency SaaS Portfolios

FedRAMP
Non-FedRAMP
Minimal Risk

EMCC
- Enterprise Demand
- Typically IaaS
- Typically FedRAMP

EMCC & Center
- Enterprise Demand
- FedRAMP (M,M,M)
- Non-FedRAMP (L,M,M)
- Minimal Risk (L,L,L)
Key Enabling Security Approach: SaaS Accreditation and Authorization

Agency (OCIO)

Agency SaaS MCE Host Center

Agency SaaS MCEs

LOW SaaS CSPs (MRP)
C, I, A = Low, Low, Low
• Minimal CSP Vetting
• Highly Tailored A&A

MODERATE SaaS CSPs
C, I, A = Low, Mod, Mod
• NIST Moderate Baseline
• Non-FedRAMP SARP
• Standard A&A Processes

MODERATE SaaS CSPs
C, I, A = Mod, Mod, Mod
• NIST Moderate Baseline
• FedRAMP SARP
• Standard A&A Processes

Security Vetting/Control Parsing Output

ConMon (via RISCS)

Primary Centers

Consuming Centers

FedRAMP SaaS CSPs

FedRAMP SaaS CSPs

Security Vetting/Control Parsing

ConMon

Common Control Source

Authorization Boundaries

User Community

Account Management
# Changes in EMCC Operating Concept

<table>
<thead>
<tr>
<th>Distinguishing Characteristics</th>
<th>Generation 1.0</th>
<th>Generation 2.0</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>Computing Services Service Office (CSSO)</td>
<td>Enterprise Managed Cloud Computing</td>
</tr>
<tr>
<td><strong>Value Proposition</strong></td>
<td>Value-added Service Provider for IaaS (AWS), governance, management oversight</td>
<td>Platform Operator and Broker that facilitates buying and selling of cloud services, governance, management oversight</td>
</tr>
<tr>
<td><strong>Customers</strong></td>
<td>NASA Managed Cloud Service Providers</td>
<td>NASA Service Providers, Projects, Communities, Individuals</td>
</tr>
<tr>
<td><strong>Platform Levels</strong></td>
<td>Wholesale</td>
<td>Wholesale, Retail (multiple levels)</td>
</tr>
<tr>
<td><strong>Service Models</strong></td>
<td>IaaS (AWS today; others planned)</td>
<td>IaaS, SaaS, PaaS</td>
</tr>
<tr>
<td><strong>Alliance</strong></td>
<td>Minimal Reliance: Business/Technical Integration and Solution Development by EMCC team</td>
<td>Extensive Reliance (planned): Scalability via the Cloud Services Delivery Network (Centers)</td>
</tr>
<tr>
<td><strong>Role of MC SPs</strong></td>
<td>Buyer, B2C Seller</td>
<td>Buyer, B2B or B2C Seller</td>
</tr>
<tr>
<td><strong>Suppliers</strong></td>
<td>CSPs</td>
<td>CSPs, NASA MC SPs, NASA Data Centers</td>
</tr>
</tbody>
</table>