



IS YOUR HEAD IN THE CLOUDS?

Forum 2017

VITA Workshop presented by:
Demetrias Rodgers, Director, Enterprise Cloud Oversight Services
Sonja Headley, Supply Chain Management, Cloud Compliance Lead



Agenda

- What is Enterprise Cloud Oversight Services (ECOS)?
- Why ECOS?
- How is ECOS different? *Data, Data, Data*
- ECOS-where and why
- Cloud responsibilities
- ECOS policy
- ECOS process
- Required ECOS procurement forms & terms
- Who can help me?
- Examples of completed ECOS assessments
- Q&A



What is Enterprise Cloud Oversight Services (ECOS)?

- Enterprise Cloud Oversight Service (ECOS) provides oversight functions and management of cloud based services, specifically focused on software as a service (SaaS). The service assures compliance and improved security by providing transparency through VITA oversight.



What is Enterprise Cloud Oversight Services (ECOS)? - continued

ECOS Applies when:

- Services under procurement meet the definition or characteristics of a SaaS provider.
- When an agency is requesting the provider to act on behalf of a commonwealth entity, is accepting commonwealth data, serving as the data custodian and/or system administrator of that data for purposes of making it available back to the commonwealth via an interface for fee.

Visit this webpage for more detail on SaaS Characteristics:

[Enterprise Cloud Oversight Services \(ECOS\)](#)



Why ECOS?

- § 2.2-2009 of the *Code of Virginia* directs VITA to provide for the security of state government electronic information from *unauthorized uses, intrusions, or other security threats* and the CIO must develop policies, standards, and guidelines (PSGs) for assessing security risks, determining the appropriate security measures and performing security audits of government electronic information. These PSGs apply to the Commonwealth's executive, legislative, and judicial branches and independent agencies.



Why ECOS? - continued

- The 2017 General Assembly session updated law to require:
 - The CIO to develop new policies, standards and guidelines (PSGs) that require that any information technology (IT) procurement by agencies be made in accordance with **federal laws and regulations pertaining to information security and privacy**.
 - VITA to implement an IT security service center to support agencies.
 - VITA's oversight of technology security and cloud based services for agencies.



How is ECOS different? *Data, Data, Data*

- Types of **Data** in the Cloud (*sensitive, PHI, PII, public*)
- Location of **Data** in the Cloud (*public, private, hybrid*)
- Access to **Data** in the Cloud
- Risks
 - Technical (*service provider platform, security, Data privacy*)
 - Supplier viability, performance and reporting
 - Contractual (*special contract terms*)
 - Loss or compromise of **Data**
 - Supplier liability
 - Return of **Data**
 - Termination/Exit strategy



ECOS – where & why

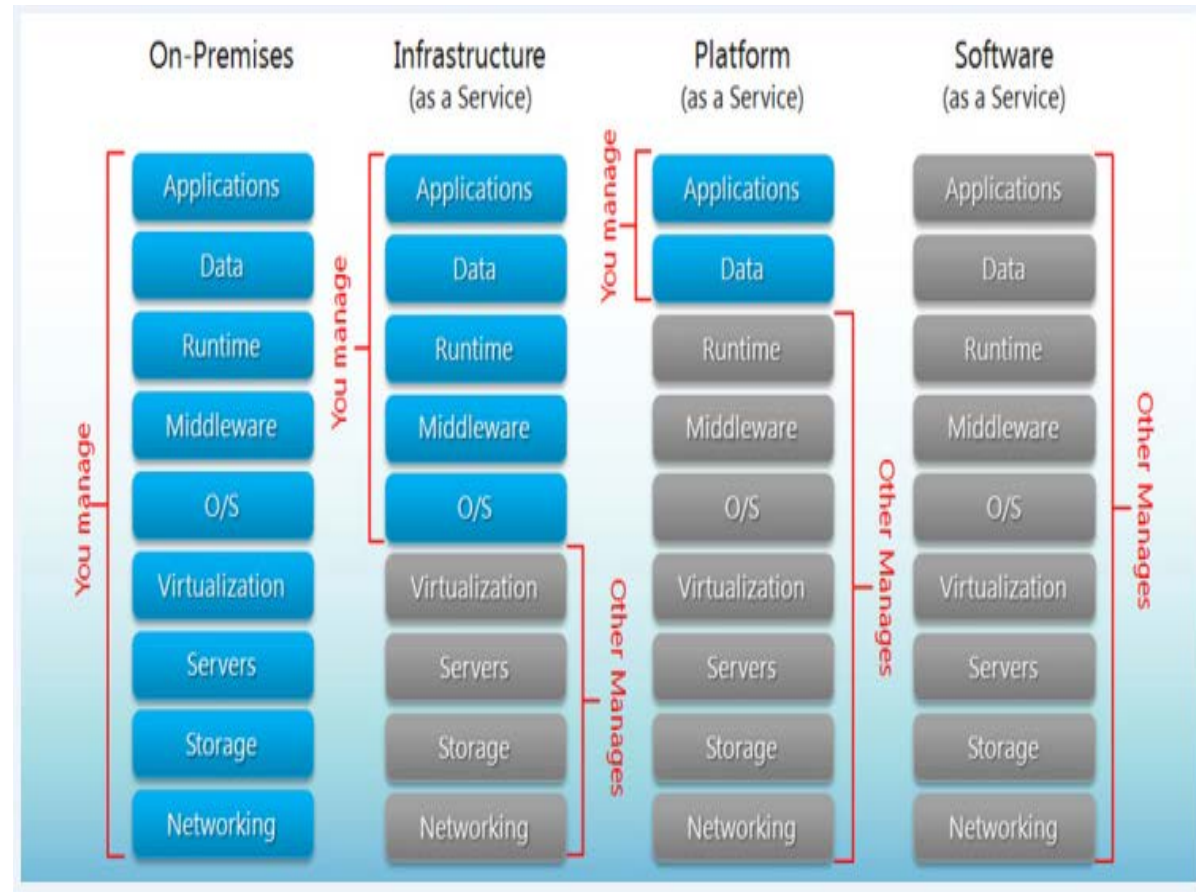
- There is shared security responsibility for cloud.
- ECOS applies for Software as a service (SaaS) only.
- There are cloud models and with each comes varying responsibility. Cloud services still require:
 - A/V, Anti-malware
 - Network security controls
 - Secure coding practices,
 - Logging, reporting and alerting.
- SaaS is the least burdensome on the agencies as well as it is the closest model to the services currently provided under our Managed Services model

Responsibility	On-Prem	IaaS	PaaS	SaaS
Data classification & accountability	Cloud Customer	Cloud Customer	Cloud Customer	Cloud Customer
Client & end-point protection	Cloud Customer	Cloud Customer	Cloud Customer	Cloud Customer / Cloud Provider
Identity & access management	Cloud Customer	Cloud Customer	Cloud Customer / Cloud Provider	Cloud Customer / Cloud Provider
Application level controls	Cloud Customer	Cloud Customer	Cloud Customer / Cloud Provider	Cloud Provider
Network controls	Cloud Customer	Cloud Customer / Cloud Provider	Cloud Provider	Cloud Provider
Host infrastructure	Cloud Customer	Cloud Customer / Cloud Provider	Cloud Provider	Cloud Provider
Physical security	Cloud Customer	Cloud Provider	Cloud Provider	Cloud Provider

Legend: ■ Cloud Customer ■ Cloud Provider

Cloud responsibilities

- Shared responsibility for security and management responsibilities are not one in the same.
- SaaS solutions are not managed by the subscribing tenant at all.
- Tenants subscribe and consume with a shared responsibility for access control related activities only for SaaS offerings





ECOS policy

- **SCOPE:** Effective 12/15/2016, the policy:
 - Applies to all agencies to which VITA provides IT services
 - Pertains to the acquisition of IT services not currently included in the services provided by VITA infrastructure and that have received all *VITA prerequisite governance approvals*



ECOS policy - continued

- **PURPOSE:** To enable the adoption of cloud-based services across the COV using VITA as an IT service provider. Cloud computing includes evaluating the service provider for adequate IT management as well as cataloging cloud services that have existing contracts with the commonwealth.
- The full policy is located here: [Third Party Use Policy](#)



ECOS process

- Demetrius will give a high-level description.
- Handouts are available if you would like one.



Required ECOS procurement forms & terms

- Administrative
- Solicitations
- Contracts





ECOS forms - Administrative

- **Memorandum of Understanding (MOU)**

The MOU is available by contacting:

Enterpriseservices@vita.virginia.gov or vitaonestop@vita.virginia.gov

- **Work requests**

- 1-003, Enterprise Cloud Oversight Service Assessment (ECOS)
- 1-004, Enterprise Cloud Oversight Service Implementation
- The work requests are available at the VITA IT Service Catalog Form Library webpage here:
<http://shop.vita.virginia.gov/default.aspx?id=6442469325>



ECOS forms - Solicitations

- ECOS assessment form
 - [ECOS Assessment Form - Attachment A to Work Request 1-003](#)
- Cloud services terms and conditions
 - Contact: enterpriseservices@vita.virginia.gov



ECOS forms - Contracts

- Cloud services terms and conditions
Contact: enterpriseservices@vita.virginia.gov
- Any ECOS approval contingencies or exceptions
 - May require a non-disclosure agreement (NDA) between supplier and agency
 - May require redaction for public facing contract
- The actual security assessment is NOT included in the contract



Who can help me?

- Your Agency Information Security Officer (ISO)
- Your Agency Information Technical Resource (AITR)
- Your VITA Customer Account Manager (CAM)
- Email to:

Enterpriseservices@vita.virginia.gov or
vitaonestop@vita.virginia.gov





Examples of Completed ECOS Assessments



Enterprise Cloud Oversight Services (ECOS)

<http://shop.vita.virginia.gov/ProductDetail.aspx?id=6442475853>

KEEP CALM and Cover Your SaaS with ECOS

KEEP CALM and Cover Your SaaS with ECOS



Executive Branch Agencies



Q&A

Now *Your* head is in the clouds!

