VIRGINIA IT AGENCY

CLOUD PROCUREMENTS AND THE ECOS PROCESS

SONJA HEADLEY AND SUSAN SIEGFRIED

VITA PROCUREMENT

TRANSCRIPT

2021

Introduction

Hello, I am Sonja Headley and this is my colleague, Susan Siegfried. We are cloud sourcing specialists in VITA's procurement directorate. In this training, we will discuss the procurement of cloud-based solutions, specifically, software as a service, or SaaS, and the ECOS process. ECOS stands for enterprise cloud oversight service and the main objective of ECOS is to protect Commonwealth data.

Note: VITA supply chain management (SCM) and procurement are used interchangeably throughout this transcript.

What are cloud based solutions?

First, we want to answer the question, what are cloud-based solutions?

Cloud-based, or SaaS solutions, are supplier-hosted, rather than on premise-hosted. Instead of downloading a SaaS application to your computer, you access it through the internet or cloud. The SaaS application runs on a provider's cloud infrastructure.

A background on ECOS

Here is some background on ECOS:

- ECOS was created in 2016 as a response to the direction of Virginia Code § 2.2-2009(A). That code section requires the Commonwealth's Chief Information Officer (CIO) to direct the development of policies, standards, and guidelines for assessing security risks, determining appropriate security measures and performing security audits of government electronic information.
- In 2018, the Governor issued Executive Order 19 that directed agencies to minimize in-house development of custom IT solutions and applications and leverage cloud solutions if recommended by VITA's cloud governance process. https://www.governor.virginia.gov/executive-actions/

A background on ECOS

- EO19 requires all cloud solutions to be governed by VITA's security and infrastructure policies, standards, and guidelines. It also says that all agency cloud solutions must be obtained through VITA's services unless otherwise approved by the CIO.

Note: Agencies have $0 delegated authority to procure cloud solutions, which means that all cloud procurements must be approved by VITA.

https://www.vita.virginia.gov/media/vitavirginiagov/supply-chain/pdf/Authority-and-Delegation-Policy.pdf

What is involved in the ECOS process?

There are three major components of the ECOS process:

1. The cloud service assessment of supplier product
2. Adequate contract language contained in the required cloud terms
3. Continuous oversight by VITA.

These three components are based on SEC525, which is the Hosted Environment Information Security Standard. https://www.vita.virginia.gov/policy--governance/itrm-policies-standards/.

While other security policies and standards apply to SaaS solutions, the primary security standard is SEC525. The purpose of this standard is to define the minimum requirements for each agency's information security management program.

The seven (7) steps in the ECOS process

We will now walk you through a high-level summary of the ECOS process and the seven (7) steps involved.

1. Check the ECOS approved supplier application list to determine whether the supplier and application have already been approved through a previous cloud service assessment.
   https://www.vita.virginia.gov/technology-services/catalog-services/enterprise-cloud-oversight-service/approved-supplier-application-list-and-ecos-metrics/
   If the supplier is already approved for the application and has remained in ECOS oversight, a new cloud service assessment is not required.

   If you have any questions about this, contact enterpriseservices@vita.virginia.gov.

The seven (7) steps in the ECOS process

2. If the supplier and the application have not been approved, or have not remained in oversight, the agency designee will download the blank “Cloud Service Assessment” form from the VITA service portal and send it to the supplier to complete and return.

   The VITA service portal is located at the following link: https://vccc.vita.virginia.gov/vita. Search for “Cloud Service Assessment” and then scroll to the bottom of the page to “Attachment for 1-003 – Appendix A” and download the form.

The seven (7) steps in the ECOS process

3. The supplier submits the completed assessment to the agency designee, who then submits it to enterprise services through the VITA service portal. Search “ECOS Assessment” or search “Service Catalog for Cloud Service Assessment,” click show more, scroll down to attach the supplier completed assessment. The system generates a task to enterprise services to conduct the assessment.

Note: The completed assessment is confidential and may never be publicly disclosed. It should be shared only with the agency procurement lead, project manager, information security officer (ISO), agency IT resource (AITR) and/or end-user, as necessary.

The seven (7) steps in the ECOS process

4. Enterprise services conducts the assessment. If additional information or artifacts are required from supplier, the Commonwealth security risk management (CSRM) cloud security architect will send the request to the agency designee to coordinate with the supplier and obtain the information. The agency designee will submit the information back to the CSRM cloud security architect by email. Once the assessment is complete, enterprise services sends an email to the agency designee with contingent approval (e.g., any resulting security exceptions and/or contractual requirements).

   The email specifies additional agency tasks (e.g., five (5) days to obtain approved security exceptions, include the contractual requirements in the cloud terms in the supplier responsibilities section). Once the assessment review is complete, the VITA cloud security architect sends an email to the agency designee with contingent approval (e.g., any resulting security exceptions and/or contractual requirements).

The seven (7) steps in the ECOS process

The email is confidential and may never be publicly disclosed. It should be shared only with the agency procurement lead, project manager, ISO, AITR and/or end-user, as necessary.

Add any contractual requirements to the cloud terms in the “Supplier Responsibilities” section, but do not include the security exceptions, as they are highly confidential and must not be publicly disclosed. Assessments are valid for twelve (12) months from approval date as long as the supplier continues to meet all security and governance requirements included in the assessment.

The seven (7) steps in the ECOS process

5. The agency designee requests the required security exception approvals from VITA security through Archer, the VITA system of record, for maintaining an agency's information related to their applications.

   The “Exception Request Form – COV IT Security Policy and Standard” is found here:

   https://www.vita.virginia.gov/media/vitavirginiagov/it-governance/psgs/docs/Blank_Exception_form.doc

   The “Archer User Manual” is found here:

   https://www.vita.virginia.gov/media/vitavirginiagov/commonwealth-security/pdf/Archer-User-Manual-2021.pdf

6. The agency designee submits a service request through the VITA service portal for ECOS oversight.

The seven (7) steps in the ECOS process

7. The agency designee or procurement lead obtains the required cloud terms ("Cloud Services – Additional Terms and Conditions") by request to: scminfo@vita.virginia.gov.

Note: No award can be made until the security exceptions have been approved by VITA and the cloud terms are in final form, with VITA approval.

Note: Even if a new cloud service assessment was not required, the agency must still request approval of the security exception(s), include the contractual requirement(s) in the cloud terms, and request ECOS oversight.

RFPs for cloud solutions

Now we are going to talk about request for proposals (RFPs) for cloud solutions.

1. First, there are a couple of prerequisite actions to perform:
    i. Determine if there is a VITA statewide contract available for your business needs, as agencies must use the statewide contracts if there is one that meets their need.
    ii. Next, you must obtain an approved procurement governance request (PGR) if the total cost of the procurement is over $250,000. The agency AITR can assist in ensuring that any other project initiation steps have been taken prior to the submission of the PGR. For more information, please view the “VITA Review Process” video under the procurement tab on the VITA website.
2. Second, include the cloud service assessment form in your RFP for suppliers to complete and submit per the instructions in your RFP.

RFPs for cloud solutions

3. Third, there is language regarding cloud procurements you should include in the RFP. VITA's RFP template includes the language. If you are not using VITA's RFP template, the language for cloud procurements can be obtained from the tool on VITA's procurement webpage called "ECOS Procedure Checklist for Cloud Solution Solicitations and Contracts." We recommend you review this checklist whenever you are doing a cloud procurement. https://www.vita.virginia.gov/procurement/policies--procedures/procurement-tools/
4. Fourth, there are cloud terms that must be included in the RFP. Request the required cloud terms by emailing: scminfo@vita.virginia.gov. It is important to have the most current version of the cloud terms because they are subject to change.

RFPs for cloud solutions

Note: All cloud solicitations must be reviewed by VITA. High-risk cloud solicitations must be reviewed by VITA and your agency's Office of the Attorney General (OAG) representative. For information on major and high-risk reviews, refer to the "VITA Review Process" training video.

If there is no RFP, you must still perform steps one through seven of the ECOS process, and ensure compliance with any other required VITA procurement policies.
https://www.vita.virginia.gov/policy--governance/itrm-policies-standards/

Note: We recommend you not use the invitation for bid (IFB) process for cloud procurements because IFBs are typically non-negotiable.

Steps to follow when awarding a cloud contract with or without an RFP

We are now going to go over the steps you follow when awarding a cloud contract with or without an RFP.

1. If there was no RFP for the cloud procurement, the agency should request a copy of the cloud terms from scminfo@vita.virginia.gov, follow the guidance comments to customize them for your agency's use, and send them to the supplier.

   If there was an RFP, the cloud terms will be in the RFP and do not need to be requested.
2. The supplier returns the cloud terms to the agency with any comments or redlines. The agency then forwards the supplier's version to the assigned VITA cloud sourcing specialist. It is in the best interest of the agency to use VITA's cloud terms only. If the supplier proposes using their own terms or a master services agreement ("MSA"), and the agency wants to consider those, VITA will recommend that the agency have its OAG representative review the MSA for conflicts and legal sufficiency.

Steps to follow when awarding a cloud contract with or without an RFP

3. The assigned VITA cloud sourcing specialist and cloud services manager review the supplier's version and provide feedback to the agency.
4. The agency schedules a negotiation meeting with their stakeholders, the supplier, VITA's assigned cloud sourcing specialist and cloud services manager. Negotiations continue until conclusion.
5. The agency submits the final version of the cloud terms to the assigned VITA cloud sourcing specialist.

Do not forget that major and high-risk contracts must be reviewed by VITA and your OAG representative.

Note: Remember, no contract can be awarded until the security exceptions have been approved, the cloud terms are in final form and VITA has approved them.

Closing

In closing, we want to thank you for viewing this training transcript. We hope you found it informative and useful to you and your agency.

If you have any questions, you may email us at scminfo@vita.virginia.gov. You may also contact enterprise services at enterpriseservices@vita.virginia.gov.

Please see the following slides for additional resources.

And just as a reminder, keep your head in the clouds!

Additional resources

- We recommend you review the "ECOS Procedure Checklist for Cloud Solution Solicitations and Contracts," whenever you are doing a cloud procurement at https://www.vita.virginia.gov/procurement/policies--procedures/procurement-tools/, (then scroll down)
- VITA's IT procurement manual, chapter 28, "Agency IT Procurement Security and Cloud Requirements for Solicitations and Contracts," at https://www.vita.virginia.gov/procurement/it-procurement-manual/chapter-28---agency-it-procurement-security-and-cloud-requirements-for-solicitations-and-contracts/
- ECOS high level process and oversight touch points at https://www.vita.virginia.gov/media/vitavirginiagov/supply-chain/pdf/ECOS-High-Level-Process-and-Oversight-Touch-Points.pdf

Additional resources

- Enterprise cloud oversight service (ECOS) at https://www.vita.virginia.gov/technology-services/catalog-services/enterprise-cloud-oversight-service/
- VITA's "Third Party Use Policy" at https://www.vita.virginia.gov/media/vitavirginiagov/it-governance/psgs/pdf/ThirdPartyUsePolicy.pdf
- Commonwealth security and cloud requirements for solicitations and contracts at https://www.vita.virginia.gov/media/vitavirginiagov/supply-chain/pdf/Commonwealth-Security-and-Cloud-Requriements-2018-07-01.pdf
- Enterprise cloud oversight services (ECOS) FAQs at https://vccc.vita.virginia.gov/vita?id=vita_kb_article&sys_id=5c059e441b43a4d0741b631ee54bcba4

Additional resources

- The training video “VITA Review Process” located on the procurement tab, of the VITA website, under the training option.
- The “VITA Procurement Approval Requirements and Processes Guide” for procurement officers and buyers at https://www.vita.virginia.gov/media/vitavirginiagov/supply-chain/pdf/VITA-ProcurementApproval-Req-Processes-Guide-for-Procurement-Officers-Buyers.pdf
- Information technology resource management (ITRM) policies, standards and guidelines at https://www.vita.virginia.gov/policy--governance/itrm-policies-standards/