Chapter 28– Agency IT Procurement Security and Cloud Requirements for Solicitations and Contracts

Chapter highlights

Purpose: This chapter provides information about the commonwealth's security and cloud compliance requirements for all agencies when procuring information technology (IT). VITA has statutory authority for the security of state government electronic information from unauthorized uses, intrusions or other security threats by developing and implementing policies, standards and guidelines, and providing governance processes and audits to ensure agency compliance.

Key points:

- Adherence to all information security policies, standards and guidelines is required of all state agencies and suppliers providing IT products or services to your agency.
- Also, any procurement of information technology made by the Commonwealth's executive, legislative, and judicial branches and independent agencies shall be made in accordance with federal laws and regulations pertaining to information security and privacy.
- In addition to VITA Security Standard SEC525 for any procurements for third-party (supplier-hosted) cloud services (i.e., Software as a Service), since agencies have $0 delegated authority to procure these types of solutions, there is a distinct process for obtaining VITA approval to procure.
- There are specially required Cloud Services terms and conditions that must be included in any solicitation or contract for cloud services and a questionnaire that must be included in the solicitation for bidders to complete and submit with their proposals.

Table of Contents

28.0 Introduction

The Virginia Information Technologies Agency (VITA), under the authority of § 2.2-2009 of the *Code of Virginia*, is directed to: ". . . provide for the security of state government

electronic information from unauthorized uses, intrusions or other security threats, the CIO shall direct the development of policies, standards, and guidelines for assessing security risks, determining the appropriate security measures and performing security audits of government electronic information. Such policies, standards, and guidelines shall apply to the Commonwealth's executive, legislative, and judicial branches and independent agencies."

VITA's statutorily-obligated security responsibilities include (but are not limited to):

- § 2.2-2009 of the *Code of Virginia* requires the Chief Information Officer of the Virginia Information Technologies Agency to develop policies, standards, and guidelines to ensure that any procurement of information technology made by the Commonwealth's executive, legislative, and judicial branches and independent agencies is *made in accordance with federal laws and regulations pertaining to information security and privacy*.
- In accordance with § 2.2-2009 of the *Code of Virginia*, VITA shall operate an information technology security service center to support the information technology security needs of agencies electing to participate in the information technology security service center. Support for participating agencies shall include, but is not limited to, vulnerability scans, information technology security audits, and Information Security Officer services. Participating agencies shall cooperate with the Virginia Information Technologies Agency by transferring such records and functions as may be required.
- Established funding for both Technology Security Oversight Services and Cloud Based Services Oversight (refer to Title 2.2, Chapter 20.1 of the *Code of Virginia*).
- In accordance with Title 2.2, Chapter 20.1, "VITA shall prioritize efforts to modernize current information technology services and to make available to agencies, where appropriate, commercially-offered information technology services including but not limited to cloud computing, mobile, and artificial intelligence."
- § 2.2-2009(C) states "[i]n addition to coordinating security audits as provided in subdivision B 1, the CIO shall conduct an annual comprehensive review of cybersecurity policies of every executive branch agency, with a particular focus on any breaches in information technology that occurred in the reviewable year and any steps taken by agencies to strengthen cybersecurity measures. Upon completion of the annual review, the CIO shall issue a report of his findings to the Chairmen of the House Committee on Appropriations and the Senate Committee on Finance. Such report shall not contain technical information deemed by the CIO to be security sensitive or information that would expose security vulnerabilities."

The CIO has given VITA's Commonwealth Security and Risk Management (CSRM) Division the responsibility for developing security-related policies, standards and guidelines, implementing them and providing governance processes and audits to ensure agency compliance. VITA's Project Management Division (PMD) and Supply Chain Management Division (SCM) and other VITA divisions participate in various oversight and governance capacities to assist CSRM in fulfilling VITA's statutory security obligations.

28.1 VITA Information security policies, standards and guidelines (Security PSGs) required in all IT solicitations and contracts

28.1.1 Application of Security PSGs to all IT solicitations and contracts

All Security PSGs are available at this URL: https://www.vita.virginia.gov/it-

governance/itrm-policies-standards/. Adherence to the Security PSGs is required of all state agencies and suppliers providing IT products or services to your agency. Agency information security officers (ISOs) or agency information technology resources (AITRs) are familiar with them.

When developing an IT solicitation or contract, the agency procurement lead must ensure the above link is included in the Technical/Functional Requirements section of the document. Use the Minimum Requirements Matrix which you can download from this SCM webpage. It is located at the first bullet under the Forms section: https://www.vita.virginia.gov/supply-chain/scm-policies-forms/.

This matrix includes usable mandatory language that points to the Security PSGs link above, as well as mandatory language and links to other VITA PSGs that cover Enterprise Architecture requirements, Data Standards requirements IT Accessibility and 508 Compliance and high risk contract requirements. Your procurement's project manager, ISO or AITR will know if any formal exceptions will be needed and will obtain any such exception from VITA, should the supplier proposal not be able to comply with any of these requirements.

In addition, if a procurement is a cloud-based procurement (i.e., off-premise hosting), Supplier's failure to successfully answer, negotiate and/or comply with any resulting security exceptions that may arise in order to approve Supplier's cloud application, may result in removal from further consideration.

28.1.2 Enterprise Cloud Oversight Services (ECOS) Security Assessments

For the ECOS Assessments, normally the Supplier will agree to any exceptions as specified by ECOS Director in his ECOS Assessment Approval. Any such exceptions would be added to the Contract. This is a standard sub-process within ECOS Security Assessment approval process. The Sourcing Consultant or procurement lead may be involved in negotiations surrounding the exceptions. Please take special note to understand the two points below:

Point 1: Because the Commonwealth has public facing contracts, the Sourcing Consultant or procurement lead may be asked to assist in obtaining Supplier's response as to whether or not the exceptions are confidential or proprietary (i.e., disclosure of these exceptions would or would not compromise the Supplier's security processes or protocols, thereby providing hackers any opportunity to hack Supplier's application or systems, or if public disclosure would or would not provide competing suppliers with too much information). If they say 'yes' then the public facing contract has to be redacted to serve your agency's responsibility to not disclose or make the information publicly available. If another agency person other than the procurement lead; i.e., business owner, project manager, ISO receives the approval from the ECOS Director, it is important that they collaborate with the assigned Sourcing Consultant or procurement lead and the Sourcing Consultant or procurement lead should follow up as a due diligence action.

Point 2: Sometimes the Supplier will ask the agency to sign a non-disclosure agreement (NDA). The ECOS Director signs an ECOS NDA, if requested by Supplier, on behalf of VITA personnel having access to the Assessment details or the Assessment responses and any resulting approval exception(s) as part of the ECOS process.

The actual ECOS Assessments are never to be included in the contract, and extreme care should be taken not to share the ECOS Assessment with non-stakeholders. Normally, the results of the ECOS Assessment and its approval and exceptions are not shared with the

Evaluation Team, as these are not evaluated per se. If a Sourcing Consultant or procurement lead needs to share, it would be wise to reiterate the confidentiality and proprietary nature of the ECOS Assessment responses and any resulting exceptions to stakeholders (in this case, meaning individuals with a need-to-know), or have stakeholders individually sign a NDA, if they have not already signed one as an Evaluation Team member.

Suppliers would not be in breach of contract compliance if they agree to comply with the exceptions and these exceptions are included in the contract, with any public facing version being redacted according to the Supplier's identification to the agency of any proprietary content. You may contact SCMinfo@vita.virginia.gov for any contractual guidance.

28.1.3 Application of ECOS policy and procedures to all Cloud Services solicitations and contracts

While agencies are required to comply with all Security PSGs as described in section 28.1.1, Security Standard SEC525provides agency compliance requirements for non-CESC hosted cloud solutions.

In addition to Security Standard SEC525, for any procurements for third-party (supplier-hosted) cloud services (i.e., Software as a Service), agencies must use this process obtaining VITA approval to procure. Refer to the Third Party Use Policy at this link: https://www.vita.virginia.gov/media/vitavirginiagov/it-governance/psgs/pdf/ThirdPartyUsePolicy.pdf.

Your agency's ISO or AITR can assist you in understanding this process and in obtaining the required documentation to include in your solicitation or contract. There are specially required Cloud Services terms and conditions that must be included in your solicitation and contract, and a questionnaire that must be included in the solicitation for bidders to complete and submit with their proposals. You may also contact: enterpriseservices@vita.virginia.gov

More guidelines for application of ECOS is available here:
Enterprise Cloud Oversight Services (ECOS): https://www.vita.virginia.gov/services/service-catalog/cloud-and-oversight-services/enterprise-cloud-oversight-services-ecos.html

Commonwealth Security and Cloud Requirements for Solicitations and Contracts:
https://www.vita.virginia.gov/supply-chain/scm-policies-forms/

ECOS Procedure Checklist for Cloud Solution Solicitations and Contracts:
https://www.vita.virginia.gov/supply-chain/scm-policies-forms/

28.1.4 Executive Order Number 19 (2018)

Executive Order Number 19 (2018), Cloud Service Utilization and Readiness, directs VITA to develop governance documents in support of the Order's cloud approach that addresses requirements for evaluating new and existing IT for cloud readiness. This process, which shall apply to Executive Branch agencies as defined in § 2.2-2006 of the *Code of Virginia*, will include details regarding the following areas:

Development of New IT Applications and Solutions

- As of the effective date of this Executive Order, all new IT solutions proposed for development must either be cloud-enabled or have a documented exemption approved by the Commonwealth Chief Information Officer (CIO).

- Agencies shall minimize in-house development of custom IT solutions and applications and leverage cloud solutions if recommended by VITA's cloud governance process.

Existing Systems/Applications Cloud Enablement

- Agencies shall evaluate the continued use of dedicated hardware supporting premise-based IT solutions.
- Agencies shall develop formal processes to enable application development and business services to evaluate cloud service options when deploying, updating, or investing in existing IT solutions.

All agency cloud solutions shall adhere to VITA security and infrastructure policies, standards, and guidelines that will be located in the ITRM Policies, Standards & Guidelines. All agency cloud solutions shall be obtained through VITA's services as outlined by the agency unless otherwise approved by the CIO.

Agency Reporting

- VITA shall collect information from each agency indicating the percentage of physical and virtually deployed IT system components as well as cloud-ready workloads.
- By December 1, 2018, and annually thereafter, each agency shall identify each system's cloud-readiness status (cloud-ready or not cloud-ready) and report this information to VITA, unless granted a temporary or permanent exemption by the CIO.
- By January 15, 2019, agencies shall provide to VITA information regarding resource requirements necessary to make systems cloud-ready within their IT strategic plans, unless granted an exemption by the CIO. This information shall be evaluated by VITA for cloud-readiness as part of the IT strategic planning process.
- By June 1, 2019, VITA shall report to the Secretary of Administration on the status of identifying cloud-ready systems within the Commonwealth.
- Beginning September 1, 2019, VITA shall report annually to the Secretary of Administration on the progress of migrating systems identified as appropriate for cloud solutions.

28.1.5 Prohibition on the use of certain products and services

Pursuant to § 2.2-5514 of the *Code of Virginia*, Commonwealth public bodies are prohibited from using, whether directly or through work with or on behalf of another public body, any hardware, software, or services that have been prohibited by the U.S. Department of Homeland Security for use on federal systems.