COMMONWEALTH OF VIRGINIA

Information Technology Resource Management (ITRM)

ENTERPRISE ARCHITECTURE STANDARD

Virginia Information Technologies Agency (VITA)

Review

This publication was reviewed and approved by VITA's Enterprise Architecture Division

Online review was provided for agencies and other interested parties via the VITA Online Review and Comment Application (ORCA).

Publication Version Control

Questions related to this publication should be directed to VITA's Enterprise Architecture (EA) Division at: ea@vita.virginia.gov *EA* PPA notifies Agency Information Technology Resources (AITRs) at all state agencies, institutions and other interested parties of proposed revisions to this document.

This following table contains a history of revisions to this publication.

Version	Date	Chapter	Section	Revision Description
EA225-00	07/10/2006	5	All	Base Document (a compilation of new and revised enterprise technical architecture standards except for the security standards).
EA225-01	10/21/2007	1		Updated Preface Provided examples for ITRM Publication Version Control Updated links Clarified glossary entries
		5	5	Updated and clarified Networking and Telecommunications
		5	6	Updated and clarified the personal computing portion Removed the prohibition of DVD writers (see change in PLA-R-08)
		5	7	Clarification of the location of the security standards
EA225-02	10/1/2008	1		Updated and clarified: the Preface and Introduction
		5	4	Updated and clarified: Integration Domain
		5	5	Updated and clarified: Networking and Telecommunications Domain
		5	7	Updated and clarified: Security Domain standards list
EA225-03	4/1/2009	1		General administrative updates to the introduction and name change from Enterprise Technical Architecture Standard to Enterprise Architecture Standard
		5	2	ETA Database Domain – updated Database and Other Data Access Methods Technology Component Standard Table DB- S-01
		5	5	ETA Networking and Telecommunications Domain – Added a topic and four (4) existing Internet Domain Naming requirements to this section. Eliminates the need for a separate standard on Virginia Government Internet Domain Naming.
		5	7	ETA Security Domain – administrative changes to reference the current versions of existing Security Standards
		5	8	Enterprise Systems Management Domain- added domain wide requirement ESM-R-23 related to standard operations tools as mandatory components of services provided.
EA225-04	6/19/2009	5	1	ETA Applications Domain has been changed to include all website related development and maintenance requirements.

Version	Date	Chapter	Section	Revision Description
				Please note that only those requirements that were added or changed from those standards are highlighted with a side bar in Section 5.1. This change and the corresponding website Topic report eliminate the need for a separate website policy, standard and guideline; and an Internet Privacy Guideline.
EA225-05	1/15/2010	1		Introduction was changed for the Glossary reference and to reflect a refined definition of "strategic" as it relates to technology standard tables. The Glossary section was removed and combined with all other ITRM IT Glossaries to create a new separate document: COV ITRM IT Glossary
		5	1	WEB-R-41 requirement corrected.
		5	6	Updated to reflect substantial changes to the Platform Domain, including new Desktop Productivity Tools Topic Report. • New requirements: PLA-R-36 through 43 have been added • New technology component standard tables PLA-S-17 through 23 have been added • Requirements PLA-R-01, 04, 05, 09, 10, 12, 14, 16, 26, 27, 28, 30, 34, and 35 have been rescinded • Technology component standard tables PLA-S-07, 14 and 15 have been rescinded
EA225-06	8/25/2010	All		Restructured standard to include "Chapters" corresponding to the high level components of the COV Enterprise Architecture.
		3		Added 11 requirements EIA-R-01 through EIA-R-11
EA225-07	04/04/2011	5	5.3	Information domain updated as follows: • New requirement: INF-R-17 • New Technology Standards Tables: INF-S-01 and INF- S-02 • Requirements INF-R-01, 02, 03, and 04 have been rescinded
		5	5.3	Electronic Records Management Topic added: • Includes 12 new requirements ERM-R-01 through ERM- R-12
		5	5.3	Health Information Exchange Topic added: • Includes 29 new requirements HIE-R-01 through HIE-R- 29
	04/04/2011	5	5.8	Enterprise Systems Management reviewed without any updates and or changes to the contents of this section.
EA225-08	10/19/2011	5	5.1	Application domain updated as follows: *Website Topic Report* updates technical requirements and recommended practices to reflect current trends in website design including the requested use of horizontal navigation, introduces social media and mobile applications, and exempts the Commonwealth of Virginia Web portal from implementing the template requirements.
		5	5.3	Information domain updated as follows: *Health Vocabulary and Interoperability Standards* have been identified by the Virginia Department of Health and the Department of General Services Division of Consolidated Laboratories as additional or modified standards for communicating data related to Electronic

Version	Date	Chap-ter	Sec-tion	Revision Description
				Laboratory Reporting, Immunizations, and Syndromic Surveillance. These standards have been reviewed and recommended for adoption by the Health Information Technology Standards Advisory Committee and are incorporated in this domain and version of the Enterprise Architecture Standards.
EA225-09	02/06/2013	5	5.6	ETA Platform Domain was updated to incorporate the requirements for mobile communications use for commonwealth owned and employee owned devices.
		5	5.1	ETA Applications Domain's Website Development topic was updated to incorporate the Website Topic Report v3's requirements addressing evolving web technology and usage with respect to Virginia common page elements, site design considerations, site content, mobile sites and mobile applications.
		5	5.4	Original ETA Integration Domain's Service Oriented Architecture (SOA) Development requirements.
EA225-10	12/23/2015	5	5.1	Updated ETA Application Domain's Website Development requirements addresses evolving Web technology including mobile websites, social media, user experience and user experience testing
	12/23/2015	5	5.5	Original ETA Networking & Telecommunications Domain's Social Media requirements
EA225-11	06/01/2016	1	1	Update necessitated by changes in the Code of Virginia and organizational changes in VITA.
EA225-12	09/21/2017	5	5.1	IT Accessibility Topic Report GOV103-02 is a complete rewrite of the GOV103-01 document to align it with the U.S. Access Board's update of Section 508 (accessibility) and inclusion of Section 255 (telecommunications) The Website Topic Report v5.0 updates and aligns the topic with the U.S. Access Board's January 18, 2017 update of section 508. The update replaces the product-based regulatory approach with an approach based on information and communication technology (ICT) functions. The update also addresses evolving Web technology.
EA225-13	01/15/2019	5	5.6	The purpose of this topic report is to provide direction on how the commonwealth will create, govern and utilize cloud-based hosting services. In accomplishing this, wherever possible and appropriate, the commonwealth has adopted or built upon international, federal/national-wide, and/or widely adopted IT guidance. This topic report applies to everyone providing and managing the provision of cloud-based hosting services for COV IT solutions, including those not considered part of the VITA enterprise.
EA225-13.1	02/04/2019	5	5.6	Administrative changes.
EA225-14	06/12/2019	5	5.5-1	Changes were made to the following requirements: SOC-R-01, SOC-R-02, SOC-R-03, SOC-R-04, SOC-R-05, SOC-R-09, SOC-R-10, SOC-R-12, SOC-R-13 and SOC-R-04

EA225-14.1	11/26/2019	5	5.6	Administrative changes to Cloud-based Hosting Services
EA225-15	10/31/2019	5	5.1	The purpose of Legacy IT Solutions (LIT) is to provide direction on how the commonwealth will migrate from legacy IT solutions to Approved IT solutions and technologies including cloud-based IT
EA225-15	*10/31/2019*	*-*	*All*	*This administrative update addresses changes in the Code of Virginia, organizational changes at VITA, abridged text and a font change to Rajdhani (heading) and Roboto (content). No substantive changes have been made to the recommended practices and/or requirements in this report.*

Identifying Changes in This Document

- See the latest entry in the revision table above
- Vertical lines in the left margin indicate the paragraph has changes or additions.
  Specific changes in wording are noted using italics and underlines; with italics only indicating new/added language and italics that is underlines indicating language that has changed.
- Note that page header dates vary throughout the document depending on when or if some portion of a particular chapter/section has been updated.

The following examples demonstrate how the reader may identify requirement updates and changes:

EXA-R-01 **Technology Standard Example with No Change –** The text is the same. The text is the same. The text is the same.

EXA-R-02 **Technology Standard Example with Revision –** The text is the same. *A wording change, update or clarification is made in this text.*

EXA-R-03 ***Technology Standard Example of New Standard –*** *This standard is new.*

~~**EXA-R-04** **Technology Standard Example with No Change –** The text is the deleted.~~

Examples of Technology Component Standard Table changes: No vertical line will appear beside updated Component Tables. Here a revision is indicated by a date and an action in the title of the table.

Table EXA-S-01: Example Table Change Technology Component Standard *Updated: [date]*
Strategic:
No change. No Change. *This is a change. This is a clarification. This is an addition.*
Emerging:
No change in this bullet and second bullet moved to strategic
Transitional/Contained:
No change
Obsolescent/Rejected:
No Change

Table EXA-S-02: Example Table No Change Technology Component Standard Reviewed: [date]
Strategic:
No change
Emerging:
No change
Transitional/Contained:
No change
Obsolescent/Rejected:
No Change

Table EXA-S-03: Example New Table Technology Component Standard New: [date]
Strategic:
New standards
Emerging:
New standards
Transitional/Contained:
New standards
Obsolescent/Rejected:
New standards

Preface

Publication Designation
ITRM Standard EA225-~~15.1~~*15.2* Enterprise Architecture Standard

Subject
Enterprise architecture implementation

Effective Date
~~06/12/2019~~ *10/31/2020*

Supersedes
COV ITRM Standard EA225-*15.2 ~~1~~ ~~02/04/2019~~ 10/31/2020*

Scheduled Review:
This standard shall be reviewed on an annual basis.

Authority

Code of Virginia, §2.2-2007 (Powers of the CIO)

Code of Virginia § 2.2-2007.1. Additional duties of the CIO relating to information technology planning and budgeting)

Code of Virginia, § 2.2-2010 (Additional powers of VITA)

Scope
This standard is applicable to all Executive Branch state agencies and institutions of higher education (hereinafter collectively referred to as "agencies") that are responsible for the management, development, purchase and use of information technology resources in the Commonwealth of Virginia. This standard does not apply to research projects, research initiatives or instructional programs at public institutions of higher education.

Purpose
This standard establishes direction and technical requirements which govern the acquisition, use and management of information technology resources by executive branch agencies.

General Responsibilities

Chief Information Officer of the Commonwealth (CIO)
Develops and approves statewide technical and data policies, standards and guidelines for information technology and related systems.

Virginia Information Technologies Agency (VITA)
At the direction of the CIO, VITA leads efforts that draft, review and update technical and data policies, standards, and guidelines for information technology and related systems. VITA uses requirements in IT technical and data related policies and standards when establishing contracts; reviewing procurement requests, agency IT projects, budget requests and strategic plans; and when developing and managing IT related services

Information Technology Advisory Council (ITAC)
ITAC advises the CIO and Secretary of Technology on the development, adoption and update of statewide technical and data policies, standards and guidelines for information technology and related systems.

Executive Branch Agencies
Provide input and review during the development, adoption and update of statewide technical and data policies, standards and guidelines for information technology and related systems.

Table of Contents

Chapter 1 - Introduction

Background

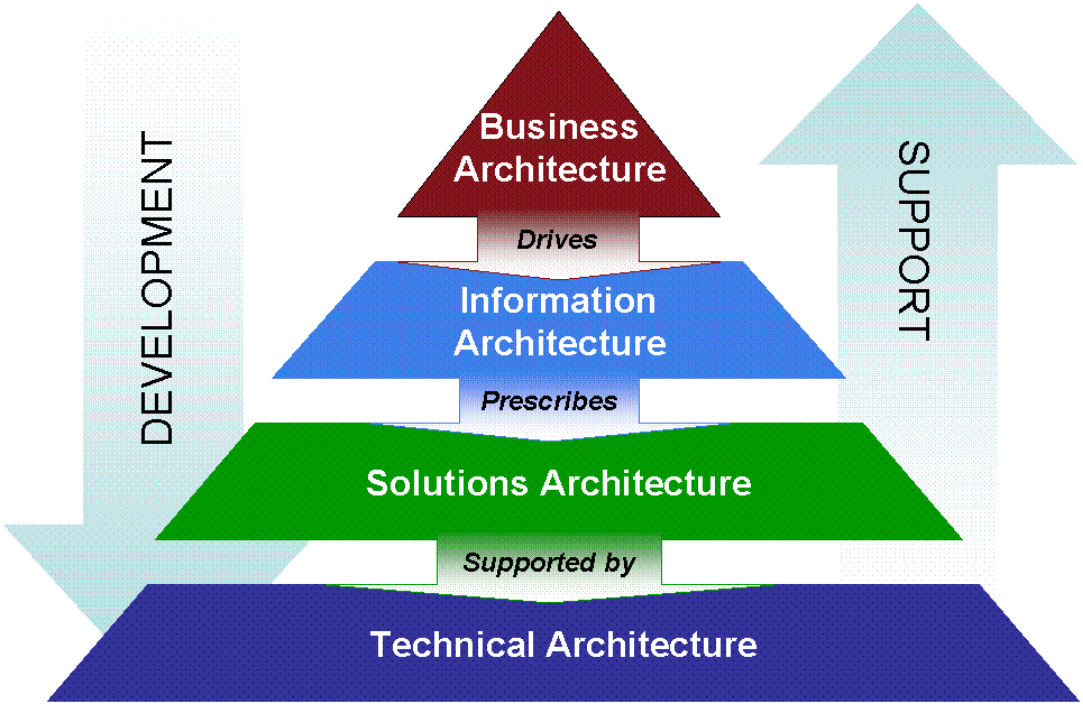
The Commonwealth's Enterprise Architecture is a strategic asset used to manage and align the Commonwealth's business processes and Information Technology (IT) infrastructure/solutions with the State's overall strategy.

The Enterprise Architecture is also a comprehensive framework and repository which defines:

- the models that specify the current ("as-is") and target ("to-be") architecture environments,
- the information necessary to perform the Commonwealth's mission,
- the technologies necessary to perform that mission, and
- the processes necessary for implementing new technologies in response to the Commonwealth's changing business needs.

The Enterprise Architecture contains four components as shown in the model in Figure 1.

Figure 1
Commonwealth of Virginia Enterprise Architecture Model



The Business Architecture drives the Information Architecture which prescribes the Solutions Architecture that is supported by the Technical (technology) Architecture.

Standard Inputs

The requirements and technology component standard tables contained in this standard have been consolidated from inputs from EA workgroups and the domain teams responsible

for researching, providing recommendations, and developing the Commonwealth's Enterprise Architecture.

Definition of Key Terms

This standard presents two forms of architecture direction for agencies when planning or making changes or additions to their information technology:

- Requirements – statements that provide mandatory Enterprise Architecture direction.
- Technology Component Standard Tables – tables that indicate what technologies or products agencies may acquire at a particular point in time. The requirements are mandatory when acquiring a new or replacing an existing technology or product. The following terms and definitions are applicable to the technology component standard tables presented in this standard:

Strategic:

This technology is considered a strategic component of the Commonwealth's Enterprise Architecture. Strategic technologies define the desired "to-be" state of the Commonwealth.

Before any updated or new Strategic technology can be deployed it must complete a formal operational review. As part of this review, agencies or vendors that provide the services needed to deploy, maintain and/or support that technology must:

- Perform the appropriate testing
- Establish the needed technical support
- Follow a formal Change Management process
- Develop any required images
- Obtain the appropriate operational reviews and approvals

In addition to the operational review, customer agencies should also:

- Perform additional testing on impact to agency specific applications
- Assess impact on business processes
- Assess training needs

The decision to deploy a Strategic technology is a business decision that is made by the agencies or vendors that provide the services needed to deploy, maintain and/or support that technology and the customer agencies. Input from the operational and customer reviews should also be included when creating implementation plans for new or updated Strategic technologies.

Emerging:

This technology requires additional evaluation in government and university settings. This technology may be used for evaluative or pilot testing deployments or in a higher education research environment. Any use, deployment or procurement of this technology beyond higher education research environments requires an approved Commonwealth Enterprise Architecture Exception. The results of an evaluation or pilot test deployment should be submitted to VITA's Policy, Practice and Architecture Division for consideration in the next review of the Enterprise Architecture for that technology.

Transitional/Contained:

This technology is not consistent with the Commonwealth's Enterprise Architecture strategic direction. Agencies may use this technology only as a transitional strategy for moving to a strategic technology. Agencies currently using this technology should migrate to a strategic technology as soon as practical. A migration or replacement plan should be included as part of the Agency's IT Strategic Plan. New deployments or procurements of this technology require an approved Commonwealth Enterprise Architecture Exception.

Obsolescent/Rejected:

This technology may be waning in use and support, and/or has been evaluated and found not to meet current Commonwealth Enterprise Architecture needs. Agencies shall not make any procurements or additional deployments of this technology. Agencies currently using this technology should plan for its replacement with strategic technology to avoid substantial risk. The migration or replacement plan must be included as part of the Agency's IT Strategic Plan.

Glossary

As appropriate, terms and definitions used in this document can be found in the COV ITRM IT Glossary. The COV ITRM IT Glossary may be referenced on the ITRM Policies, Standards and Guidelines web page at: *https://www.vita.virginia.gov/it-governance/glossary/*

Agency Exception Requests

Agencies that want to deviate from the requirements and/or technology standards specified in this standard may request an exception using the *Enterprise Architecture Change/Exception Request Form.* All exceptions must be approved prior to the agency pursuing procurements, deployments, or development activities related to technologies that are not compliant with this standard. The instructions for completing and submitting an exception request are contained in the current version of *COV ITRM Enterprise Architecture Policy.* The Policy and exception request form can be found here: https://www.vita.virginia.gov/it-governance/enterprise-architecture/ea-change-exception-requests/

Chapter 2 - Enterprise Business Architecture - EBA

The EBA documents the business strategy, governance, organization, and business functions of Virginia state government, and identifies which organizations perform those functions. The EBA provides a look at the big picture of state government from a business perspective to define who we are, what we do, and where we want to go.

The Enterprise Business Model (EBM) of the EBA was developed to define the "what we do" in terms of business functions independent of the organizations that perform those functions. That model was developed from the Federal Enterprise Architecture's Business Reference Model and was validated through workshops of agency business leaders. These workshops mapped individual agency business functions to the EBM, thus creating the Commonwealth's as-is business architecture for Executive Branch agencies.

For additional information, readers can use the EBA application or consult published EBA reports which can be found on the COV EA website at: https://www.vita.virginia.gov/media/vitavirginiagov/it-governance/ea/pdf/EBAReport.pdf.

There are no EBA Requirements or Technology Component Standard Tables at this time.

Chapter 3 - Enterprise Information Architecture - EIA

Government and government services are normally information driven. Government organizations constantly and dynamically gather and process data to create information needed to support their missions, whether it is disaster recovery, environmental protection, citizen security, or other direct services. The Enterprise Information Architecture (EIA) provides the framework/model and methodology that will enhance each agency's ability to quickly discover, access, and understand data and create the information needed to make critical decisions and support agency business functions.

The EIA is designed to provide a common framework for the cost effective sharing of government information across organizational lines while respecting the security, privacy and appropriate use of that information. It must enable agency leaders to manage information as a Commonwealth asset to better serve the citizens of Virginia. It increases the Commonwealth's agility in drawing out the value of information as a strategic mission asset.

For a more comprehensive understanding of the commonwealth's Enterprise Information Architecture, readers are encouraged to read the published EIA report, which can be found on the COV EA website at: http://www.vita.virginia.gov/oversight/default.aspx?id=365.

EIA Requirements

Data management is highly decentralized in the Commonwealth, yet there are considerable amounts of commonly used data that if standardized, could increase data sharing and interoperability between systems and governmental programs. In order to implement data standards, the Commonwealth needs a defined process for how to standardize data.

EIA-R-01 **Data Standardization Process –**VITA shall develop and maintain a defined process for how to standardize enterprise data.

A **data asset metadata repository** is a system that contains information that describes at a high level the data assets that comprise the collective data assets of the Commonwealth. The Commonwealth Enterprise Technology Repository (CETR) provides the means to maintain an inventory of the Commonwealth's data assets. It can be accessed by authorized users here: https://ssl01.apps.vita.virginia.gov/CETR/default.aspx. Access may be requested by sending an email to ea@vita.virginia.gov.

EIA-R-02 **Data Asset Repository Maintenance –** Agencies shall maintain a current inventory of the data assets used by their application portfolio as part of the Commonwealth's Enterprise Technology Repository (CETR).

A **data standards catalog** contains the instances of metadata associated with individual data standards (i.e. procurement), entities (i.e. vendor or customer) associated with each individual data standard, and attributes (i.e. vendor name or vendor ID) associated with each individual entity. The catalog does not store the actual information but rather describes how attributes about an entity related to a specific data standard are to be collected, stored, and shared.

EIA-R-03 **Data Standards Catalog –** Approved Commonwealth data standards shall be posted to the COV Data Standards Catalog.

A data standard represents a set of requirements related to a specific subject area that define how associated data is to be collected, stored, and exchanged. At a minimum, a data standard must include a narrative describing the implementation requirements and corresponding time lines for agencies. A data standard may also include artifacts such as data models, data dictionaries, and implementation specifications.

EIA-R-04 **Data Standard Narrative –** Approved Commonwealth data standards shall contain a data standard narrative that at a minimum defines the implementation requirements and corresponding time lines.

Executive branch agencies are required to use the COV Data Standards Catalog as follows:

EIA-R-05 **Implementation –** Agencies shall comply with the implementation requirements of all approved Commonwealth data standards.

EIA-R-06 **Migration –** Agencies shall assess the impact of all approved COV data standards on their existing processes and applications and define migration strategies for implementation.

EIA-R-07 **New Projects and Major Enhancements –** Agencies shall review the Data Standards Catalog when developing plans for new applications or major enhancements to existing applications and document the potential impact of implementing existing data standards on the planned project.

EIA-R-08 **Develop New Standards** – Agencies shall work with VITA to develop internal enterprise data standards and/or identify external enterprise data standards for their domain of expertise (e.g. Finance, Licensing, etc.).

EIA-R-09 **RFP/RFI/IFB and Contract language –** All Request For Proposals (RFP), Requests For Information (RFI), Invitation For Bids (IFB), and contracts that concern IT software solutions shall contain text that requires any solution to be compliant to the COV Data Standards or have an approved Data Standard Exception.

EIA-R-10 **Data Standards Catalog –** VITA shall maintain and manage the Data Standards Catalog.

Over time, data standards can become out of date and no longer accurately reflect the needs of the business. In order to ensure that data standards are current they must be reviewed on a periodic basis by the business owners. This is particularly important for the narrative that is required for each data standard. The narrative contains information about implementation plans and compliance schedules. This type of information will need to be updated as needs change and plans progress.

EIA-R-11 **Data Standard Review –** Designated Data Standard Owners shall review Data Standards annually. An update to the Narrative for each Data Standard shall be made certifying that the Narrative and any accompanying models are accurate and current.

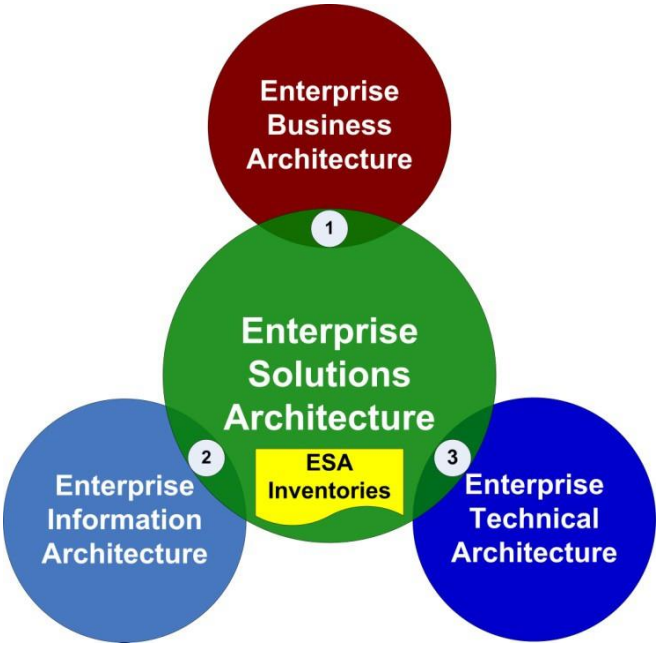
Chapter 4 - Enterprise Solutions Architecture - ESA

The expectations of government to deliver more services, to deliver them better, and more cheaply, presents a challenge for the Commonwealth. Well-engineered automated solutions[1] can increase productivity in service delivery to help meet these expectations.

Commonwealth agencies make significant investments in these automated solutions in order to carry out the business of Virginia government.[2] The Commonwealth Enterprise Solutions Architecture (ESA) provides the framework/model and methodology that supports the transition from silo-based, application centric and agency centric information technology investments to an enterprise approach where solutions are designed to be flexible. This allows agencies to take advantage of shared and reusable components, facilitates the sharing and reuse of data where appropriate, and makes the best use of the technology infrastructure that is available.

The ESA needs to contain a unified view of solutions to achieve this increase in reuse and the reduction of solution complexity. To support this, the framework/model and methodology includes: inventories, governance/guidance, and the relationships between agency applications and the other EA component architectures.

Figure 2
Commonwealth of Virginia ESA: Unified View of Solutions



The unified view of solutions includes the Business (EBA), Information (EIA) and Technology (ETA) perspectives. This view also shows how agency solutions/applications connect to:

[1] A solution is an implemented system that solves a business problem. A solution is much more than any application software it may incorporate: It includes infrastructure, people and any other aspects necessary for a business problem to be solved. [Gartner: Enterprise Solution Architecture: An Overview; Bruce Robertson; 6 June 2008 ID Number: G00157412]
[2] Derived from: Commonwealth of Virginia Strategic Plan for Applications; DRAFT 3/11/09

1. Data The business of the Commonwealth - by sub-lines of business Assets - by
2. Data Exchanges
3. Infrastructure Services - by Software Tools (Operating Systems, Languages, etc.)

Additional information on the Commonwealth ESA will be provided in the ESA Report[3]. When published, this report will be found at: https://www.vita.virginia.gov/it-governance/enterprise-architecture/ea-library/

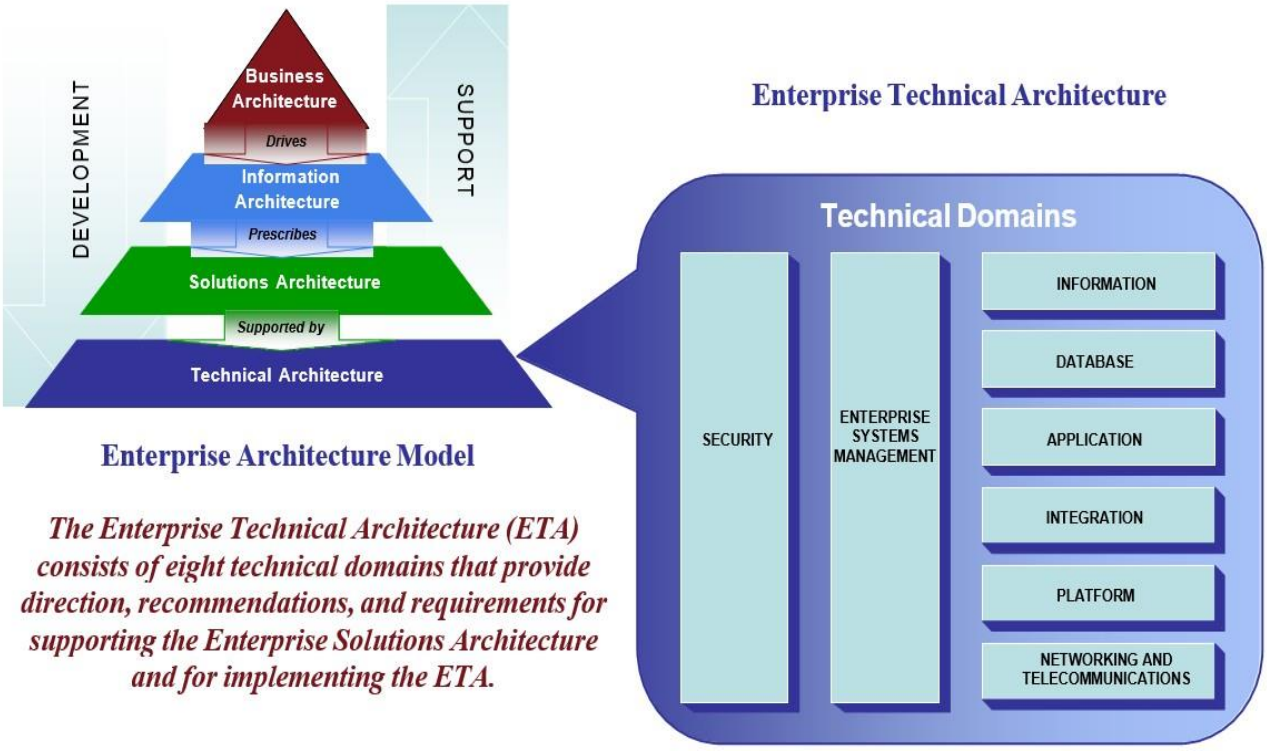
There are no ESA Requirements or Technology Component Standard Tables at this time.

[3] Scheduled for publication in 2nd quarter of 2010

Chapter 5 - Enterprise Technical Architecture - ETA

The Enterprise Technical Architecture (ETA) shown in Figure 3 consists of eight technical domains that provide direction, recommendations and requirements for supporting the Solutions Architecture and for implementing the ETA. The ETA guides the development and support of an organization's information systems and technology infrastructure.

Figure 3
ETA Relationship to the Enterprise Architecture



Each of the domains is a critical piece of the overall ETA. The Networking and Telecommunications and Platform Domains address the infrastructure base and provide the foundation for the distributed computing. The Enterprise Systems Management, Database, Application, and Information Domains address the business functionality and management of the technical architecture. The Integration Domain addresses the interfacing of disparate platforms, systems, databases and applications in a distributed environment. The Security Domain addresses approaches for establishing, maintaining, and enhancing information security across the ETA.

Section 5.1 - ETA Applications Domain

The Commonwealth relies heavily on computer applications to support agency business operations. The agencies' business processes often must change in response to both legislation and new demands from citizens. Unfortunately, the Commonwealth's computer applications cannot always respond to these changes in an effective and efficient manner because many current applications are either monolithic or two-tier client/server applications.

Many of the Commonwealth's current applications/solutions were developed independently using different languages and tools. The ability to communicate with other applications or systems or to adapt to changes in the business processes generally was not a design requirement. This architectural approach has adversely impacted the Commonwealth's business in three ways:

1. Additional cost and time needed to modify existing applications to support changing business requirements
2. Difficulty in integrating applications to share common services and data
3. Extra expense to develop, use, and maintain new applications because there is little reuse of code between applications

Application development tools, methodologies and technology are now available that can help address these problems. Examples include:

- Reuse of Code: Units of code previously duplicated in many applications can be packaged into components or services for reuse in different applications.
- Integration tools/Middleware: Shared software allows applications to communicate with each other, access data residing on different platforms, and access shared services.
- New User Interface Options: There is an expanding array of user interface options - including Web browsers, personal digital assistants (PDAs), and interactive voice response units (IVRs).
- N-tier Service-Oriented Architecture (SOA): In the n-tier SOA, applications are partitioned into discrete functional units called "services." Each service implements a small set of related business rules or function points. If a business rule must be modified to support changing business requirements, only the service that implements that business rule is impacted. The remainder of the application remains intact. The SOA comprises loosely coupled (joined), highly interoperable application services that interoperate over different development technologies. The services are very reusable because the interface definition is defined in a standards compliant manner.

The ETA Application Domain provides agencies with a foundation of development and support platforms, tools, processes, practices and requirements that can implement business processes and meet the Commonwealth's ever changing business needs.

Topic-wide Requirements

The following domain-wide requirements pertain to all topics and components in the Application Domain:

APP-R-01 **Security, Confidentiality, Privacy and Statutes –** Agencies shall implement applications/solutions in adherence with all security, confidentiality and privacy policies and applicable statutes.

APP-R-02 **Software Tools Version/Release Support –** The version/release levels of all software tools used for development and support of Commonwealth and/or agency "*mission critical applications*" shall have vendor or equivalent quality level support available.

APP-R-03 **Disaster Recovery and Business Continuity Planning –** An assessment of business recovery requirements is mandatory when acquiring, developing, outsourcing, or making major enhancements to "*mission critical applications*". Based on that assessment, appropriate disaster recovery and business continuity planning, design and testing shall take place.

APP-R-04 **Maintain Software Tools Inventory –** VITA shall collect data on agency (excluding higher education) use of software tools, maintain an up-to-date inventory, and perform research in order to create a more effective and efficient environment in support of the Application Domain.

Enterprise System Design

Enterprise System Design refers to a collection of technologies, practices, requirements and standards that can assist the agencies in the design of solutions that can meet the Commonwealth's ever changing business needs.

Service Oriented Architecture (SOA): Implementation and Governance

In a Service-Oriented Architecture (SOA) environment, nodes on a network make resources available to other participants in the network as independent services that the participants access in a standardized way. Unlike traditional object-oriented architectures, a SOA comprises loosely coupled (joined), highly interoperable application services. Because these services interoperate over different development technologies (such as Java and .NET), the software components become very reusable due to the virtue of the interface definition being defined in a standards compliant manner (Web Service Definition Language [WSDL]). This also encapsulates and hides the vendor/language specific implementation from the calling client/service. SOA provides a methodology and framework for documenting enterprise capabilities and supports both integration and consolidation activities.

SOA-based composite applications will enable the Commonwealth to integrate business- critical processes with existing applications and systems. To gain the agility, flexibility and efficiency that SOA enables, these services and composite applications must be accessible and controlled across the enterprise.

The Commonwealth needs to implement a SOA as a foundation for Enterprise Applications and agency developed solutions for in-scope agencies. A key to successful implementation is SOA Governance.

SOA Governance is the ability to ensure that all of the independent efforts (whether in the design, development, deployment, or operations of a Service) come together to meet the enterprise SOA requirements

APP-R-05 **Implement SOA** – Agencies excluding higher education shall create and implement the centralized architectural review processes that are needed to support and control SOA implementation ensuring that all services built

conform to standards, are interoperable, non-duplicative, and reusable where possible.

APP-R-06 **SOA Support of .NET and J2EE (Java Platform Enterprise Edition) –** The Commonwealth's SOA for in-scope agencies shall support both .NET and J2EE Enterprise Framework Platforms.

APP-R-07 **SOA Center of Excellence Review of Developed Applications –** VITA, together with other executive branch agencies, shall create recommended practices and requirements to implement the SOA Center of Excellence enterprise level (state-wide excluding higher education) architectural design review and architectural governance of agency developed new applications that are large-scale, complex, use/create web services, or can potentially share business processes with other agencies.

APP-R-08 **SOA Center of Excellence Review of COTS (Commercial off- the-shelf) –** VITA, together with other executive branch agencies, shall create Enterprise level (state-wide excluding higher education) architectural review recommended practices and requirements to support agency's review/selection and implementation of COTS based solutions that implement Enterprise-wide Applications or cross-cutting functions (such as accounting, facilities management or procurement).

Enterprise Artifact Repository

Agencies should consider the reuse of existing applications and system components/artifacts first, as part of their systems acquire/develop decisions. To be successful, a state-wide library (repository) of reusable components and artifacts must be implemented and maintained.

Designers can build flexible, scalable, and extensible applications by using components as application building blocks, similar to building cars on an assembly line. Using previously built and tested components in different ways or with new components can accelerate the design, development, and delivery of new applications. Sharing of components across applications can also eliminate significant duplicate design and test efforts.

There are two strategies for reuse:

1. Opportunistic reuse: using assets that were not designed to be reused or are reused in a manner for which they were not designed
2. Systematic reuse: using assets which were purposefully designed, built, and managed to be reused

   Systematic reuse has several advantages:

   - Responsiveness: accelerates and streamlines project delivery
   - Return on Investment (ROI): reduces solution delivery costs and provides only those assets that produce the best business advantage
   - Quality: ensures that only quality assets will be reused

Both reuse strategies require an implemented Enterprise Artifact Repository with supporting practices and processes to be successful.

APP-R-09 **Implement Enterprise-wide Artifact Repository –** The Commonwealth shall select, deploy and maintain an Enterprise- wide Artifact Repository to

support implementation of a SOA and create recommended practices and processes that support and encourage agency use of the Repository.

Application Acquisition

The choice of a systems acquisition method (buy/build decisions) should take into account the functional characteristics of the proposed systems. The agencies should first consider the reuse of existing applications and system components. If no components exist, purchased solutions (COTS) should be explored. Applications or systems that can provide automation of agency core business functions that have unique processes, yield competitive advantages, or have demonstrable cost savings and/or enhanced value should be the only candidates for in-house development by the Commonwealth.

Commercial off-the-shelf (COTS)

Commercial off-the-shelf (COTS) is a term for software or hardware products that are ready-made and available for sale to the general public. They are often used as alternatives to in-house developments or one-off government-funded developments (government off-the-shelf [GOTS]). The use of COTS is being mandated across many government and business programs because they may offer significant savings in procurement and maintenance.

APP-R-10 **Evaluate COTS as Alternative** – Commercial off-the-shelf (COTS) solutions shall be evaluated and documented as part of an Alternatives Analysis of systems acquisition methods for all Enterprise-wide Applications and cross-cutting functions (such as accounting, facilities management or procurement).

APP-R-11 **COTS Documentation –** All "mission critical" COTS solutions shall have their application components and configurations fully documented.

Development and Support Platforms

The complexity, size, lifespan, and performance requirements of agency developed applications/solutions vary greatly. Development and Support Platforms provide the agencies with distinct approaches to address different application needs/ requirements.

These approaches can be implemented by the following development platforms:

- Enterprise Framework Platform – supports n-tier development of service-oriented architecture for large-scale or complex applications that need to support high-volume usage and/or long life spans.
- N-tier Visual-based Tool Development Platform – supports applications that are not large-scale, complex and do not require high-volume usage and/or long life spans. Generally developed by Business Analysts by using visual-based tools that provide automated code generation.
- Collaborative Platform – many business' needs do not require scalable or highly available solutions. These needs often can be met by Workflow and Forms Automation tools.

Development Languages

There have been thousands of different programming languages and new ones are created every year. Every language has its strengths and weaknesses. For example, FORTRAN was (and still is) a particularly good language for processing numerical data, but it does not lend itself very well to organizing large programs. Pascal was very good for writing well- structured and readable programs, but it is not as flexible as the C programming language. C++ embodies powerful object-oriented features, but it is complex and difficult to learn.

The Commonwealth will continue to use specialized development languages as required to meet special needs (example: FORTRAN for engineering applications). With the exception of these special needs applications, in-house development should use languages that are consistent with the creation of SOA n-tier solutions on Enterprise Framework Platforms such as .NET and J2EE.

Table APP-S-01: Languages used in developing new large, complex applications anticipated to have high usage volumes and/or long life spans Technology Component Standard
Strategic:
Java, Visual Basic, C++, VB.NET Fortran (for engineering applications only)
Emerging:
Transitional/Contained:
Cobol, Power Builder, PL/SQL, Delphi, MAPPER (BIS, Cool Ice)
Obsolescent/Rejected:
Assembler, C, Clipper, Basic, PL/1

Coding Guidelines and Standards

Coding Guidelines and Standards (also called programming style or code convention) describe conventions for writing source code in a given programming language.

APP-R-12 **J2EE and .NET Guidelines –** The Commonwealth shall research and publish recommended practices supporting agency development of applications/solutions using J2EE and .NET Enterprise Frameworks.

Software Engineering

Software Engineering is the application of best-practice processes and methods of design to the development and maintenance of software applications/solutions. Software engineering

covers not only the technical aspects of building software systems, but also development management issues, such as testing, modeling and versioning.

APP-R-13 **Commonwealth Web and Accessibility Standards** – Public- facing and Web applications (Intranet and Internet) shall comply with Commonwealth Web and Accessibility Standards as applicable.

APP-R-14 **Public Web Applications Browser Independent –** Agency public-facing web-based solutions shall be browser independent (the functionality of the application can not be restricted to a single browser)

APP-R-15 **Maintain Application Code Documentation –** All newly developed applications shall have their code documented. This documentation shall be maintained throughout the product life cycle.

APP-R-16 **Accessible and Transferable Repositories –** All electronic repositories of source code, metadata, development artifacts, models, documentation, etc. shall have their contents accessible either by an export facility or direct access method. This ability is required to allow the repository contents to be transferred from one methodology or tool to another as needed.

Reusable Components/Artifacts

A component is a loosely defined term for a software technology for encapsulating software functionality. Components must meet the following five criteria:

1. Multiple-use
2. Non-context-specific
3. Combinable with other components
4. Encapsulated i.e., non-investigable through its interfaces
5. A unit of independent deployment and versioning

An artifact is a valuable, high quality software work product such as: documentation, analysis and design models, source code, interfaces, executable binaries, tools, processes, and test plans. To be successful, agencies must be able to search for existing applications, components and artifacts that have already implemented specific business processes.

APP-R-17 **Search for Existing Business Process –** The Commonwealth Enterprise Architecture shall evolve to incorporate a search feature that addresses the customer's need to locate existing Commonwealth/ agency (excluding higher education) solutions that implement specific business processes.

Configuration Management

Configuration Management is applicable to all aspects of software development from design to delivery. It focuses on the control of all work products and artifacts generated during the development process. Version Management (a subset of Configuration Management) refers to the tracking and controlling of file versions. It includes capabilities such as labeling, branching, merging, version content comparisons, and security and permission management. An initial step on the path to Configuration and Version Management is to implement a source code repository with supporting processes.

Code management is crucial to maintain application integrity through the development and maintenance

lifecycle. Ideally, code management tools would integrate with defect tracking and application-build tools. The Commonwealth will be researching code management systems that can scale across the enterprise to foster an environment that supports reuse of shared components.

APP-R-18 **Source Code Repository –** All application source code shall be maintained in a repository using a formal process.

Website Development

The website requirements presented below encourage greater efficiencies and effectiveness in the use of technology, and provide guidance and direction to assist agencies in developing a common look and feel to agency public websites. The templates and requirements related to implementing those templates provide basic rules of proper website design and address accessibility, template, portal, and implementation requirements and agency plans for implementing those requirements. This includes items to be addressed on every agency web page; site and application content to be included on every agency Website; design considerations for every agency website; external content to be included on every agency website; and the implementation and the World Wide Web Consortium (W3C), 2.0 considerations for every agency.

All Executive Branch agencies' public websites and public web applications (except as noted in WEB-R-05) must comply with the WEB-R requirements below. Extranets and Intranets are not required to follow the WEB-R requirements, but still must comply with the current version of the COV ITRM *Accessibility* Topic Report (GOV103).

Virginia Common Template - Page Elements

These elements provides a common web template and corresponding guidance and direction related to all the components an agency must put on every page of its website.

An important objective of the Common Template Requirement is to create a user-focused, or "user-centric," web presence for the Commonwealth, including a common look and feel to all agency websites. This objective is addressed by creating a template and set of website requirements for all agencies to implement that assist in making the agency web pages accessible and usable. An essential objective of this requirement is to assist in making the Web site user's experience as pleasant and trouble-free as possible. It also includes putting government services and content where citizens can easily find them, and in a format that is easy to use.

Code containing the "Commonwealth Banner," all links contained within the banner, sample template code and specifications are located at the VITA site: http://www.developer.virginia.gov.

Commonwealth Banner

The Commonwealth Banner is the black bar that appears at the top of Virginia government web pages. It contains links relevant to all agencies.

WEB-R-01: **Commonwealth Banner Code, Content and Location**

Agency Sites
The code containing the "Commonwealth Banner" shall be used on all agency websites and is available on the VITA site at: http://www.developer.virginia.gov.

- "Skip to Content" – (skip-nav) shall be hidden within the code of the Commonwealth Banner to allow screen reader access at the beginning of each page.
- "Find an Agency" – right align text link

- "Virginia.gov" – right align text link
- The "Commonwealth Banner" shall be ~~black and~~ posted above the "Agency Header" ~~area~~ at the top of every page of each site. It shall be *28* ~~40~~ pixels in height in its default mode.

Mobile Display

- On mobile display's home page, the Commonwealth Banner shall be posted above the agency header at the top at least 15 pixels high.
- The virginia.gov logo shall link to the Virginia.gov portal.
- The other standard site Commonwealth Banner requirements are optional for mobile display.
- On subpages, the Commonwealth Banner is optional. If the Commonwealth Banner is not shown, the Virginia.gov logo shall appear in the page footer.
- For the definition of Mobile Display and Mobile App see Key Definitions above.

Virginia.gov Portal

The Virginia.gov portal shall comply with the most recent requirements in the Website Topic Report, except as noted herein.

The Virginia.gov portal website shall comply with the WEB-R-01 requirements except instead of the Virginia.gov logo, the Virginia.gov Commonwealth Banner shall have the text "The official website of the Commonwealth of Virginia" left-aligned.

Virginia Common Template

The Virginia Common Template is a visual arrangement of Web page elements. It specifies where common items shall appear so users know where to look for them and to have a unified look-and-feel across Virginia government websites.

WEB-R-05 **Virginia Common Template –** All Executive Branch Agencies shall use the Virginia Common Template for public websites and Web applications, except the following exempt organizations:

- The Virginia Tourism Corporation
- The Library of Virginia
- All museums
- All institutions of higher education

Extranets and intranets are not required to follow any website requirements but still shall comply with the current version of the COV ITRM *IT Accessibility Topic Report* (GOV103-0*1*).

All requirements in the *Website Topic Report* apply to both the primary agency website and the mobile version, except as noted herein.

.

Site Banner

The Site Banner is the area below the top black Commonwealth Banner and above the Navigation Trail. It contains the agency name and often contains graphics related to the agency.

WEB-R-07: **Agency Header** – Each agency shall create its own Agency Header for use in the template; it shall be 100 pixels high and able to accommodate screen resolutions 1366 and wider gracefully.

- The Agency Header shall contain the full agency name or site name and be created in one of the specified standard fonts.

Mobile Display

- For mobile display, there shall be an Agency Header. It has no height requirements.

- The mobile Agency Header is required on all subpages. The Agency Header shall identify the agency by containing the approved agency name, site name, agency abbreviation, or logo. A "Back" or "Menu" link shall be displayed in the Agency header on any page that does not explicitly list the main Agency Header navigation links.

Other items, design or functional, may be used in this area based on each agency's business needs.

WEB-R-43: **Enterprise and/or mandated graphic and other independent links** – Enterprise and/or mandated graphic and other independent link shall be prominent and visually separated and below the navigation links to avoid user confusion and do not count towards the 12-link limit. Examples include graphic links to agency-specific reports on Commonwealth Data Point. These graphic links should be clearly delineated from the primary navigation to assist the user; they may or may not appear on each page beyond the home page, as determined by the agency. The Virginia Information Technologies Agency (VITA) must approve exceptions prior to site redesign implementation.

WEB-R-08: **Site Search –** If a site contains more than 36 pages it shall provide an agency site search box which must appear on every page and be located in the upper right quadrant of the page but not in the Commonwealth Banner.

Mobile Display

- If the mobile site contains more than 36 pages, the mobile version shall also provide a search feature. Placement is at the discretion of the agency.

Breadcrumb Trail

The "Breadcrumb Trail" appears below the "Agency Header." It shows the route from the homepage to the page the user is on. Using the Navigation Trail links, users can return to previous or parent pages. The links can help orient a user.

The following are requirements related to Breadcrumb Trails:

WEB-R-09: **Breadcrumb Trail Location** - A Breadcrumb Trail shall be located below and contiguous to the "Agency Header" in the template. If the primary navigation is horizontal, the Breadcrumb Trail shall be placed immediately ~~above or~~ below the primary navigation.

The breadcrumb text shall be located on the left side of the navigation bar. See Glossary: "breadcrumb"

Mobile Display

- For mobile display, the Breadcrumb Trail is optional.

WEB-R-11 **Breadcrumb Trail Height & Resolution –** The Breadcrumb Trail shall not exceed 25 pixels in height in its default mode. This area shall be permitted to grow to accommodate changes in font sizes through user specification or scripting such as CSS and/or JavaScript that allow font sizes to change. This section shall be scalable, but always default to no more than 25 pixels in height with standard font sizes. If breadcrumb text wraps to a second line, the breadcrumb bar can become taller to accommodate it.

Mobile Display

- For mobile sites, there are no requirements for Breadcrumb Trail Height and Resolution.

Navigation Links

Navigation Links refer to the main links on the left side or top of agency Web pages. They generally link to major areas or categories on a site.

WEB-R-14 **Primary Navigation Links**

- If the primary navigation is vertical, it shall be located on the left side of the page immediately below the "Breadcrumb Trail."
- If the primary navigation is vertical, no more than twelve main navigation links shall be used.
- If the primary navigation is in the Agency Header, it shall be placed immediately above "Breadcrumb Trail."
- If the primary navigation is horizontal, no more than eight main navigation links shall be used.
- If the primary navigation is vertical, the Breadcrum Trail shall be above the main page content.
- If top navigation with dropdowns is used, the dropdowns may temporarily overlap the Navigation Trail and content area as long as the dropdowns can be closed so users can access the Navigation Trail and content area.
- If a site uses both a left column of navigation and a top navigation bar, the primary links shall only appear in one of the two locations. A site may have (but is not required to have) both a left column of navigation and a top navigation bar.
- Primary links shall remain the same throughout the site.
- Graphics and other links on the left side of the page shall be visually separated and below navigation links to avoid user confusion.
- The Virginia Information Technologies Agency shall consider approval of requests for exceptions prior to site redesign implementation.

Mobile_Display

- A mobile site's primary navigation shall appear immediately above or beneath the Breadcrumb Trail (if any). If there is no Breadcrumb Trail ~~Bar~~ then the primary navigation shall appear under the Agency Header.

- On subpages, the Primary Navigation may be replaced with a link to the mobile site homepage or evoked from the Menu button.

  - Mobile displays do not need to include all of the navigation links from the primary agency website.

  - Mobile displays do not need to contain all the content from the primary agency website.

- Mobile displays may have a collapsible menu.

WEB-R-15 **Number of Sub-navigation Links –** There shall be no more than twelve sub-navigation links for a primary navigation link. Sub-navigation shall be visually distinct from the main navigation links (e.g., indented, fly-out, different color or different location). Sub-navigation links shall be semantically distinct from the main navigation links. Sub-navigation links shall not count towards the primary navigation link limit, and may vary from page to page.

Page Footer

The Page Footer is the area at the bottom of an agency Web page. It contains specific standard information about the site.

WEB-R-17 **Page Footer** - Each page shall have a footer containing, at a minimum, the following information:

- Agency name
- Copyright information
- Text or an approved icon link stating WAI compliance
- Link to the agency's Internet Privacy Policy Statement.
- "Contact Us" link (Agencies may add other "Contact us" links as desired; only this one is mandated.)

Mobile Display

- For mobile display subpages without the Commonwealth Banner, the Virginia.gov logo shall appear in the page footer.

Contact Instructions

Contact Instructions provide information to visitors that enable them to contact the agency for help, for example by phone or e-mail.

WEB-R-19 **Contact Instructions –** The Contact Us page, accessible from the home page and shall include, at a minimum, the agency's:

- Mailing address;
- FAX number, if available;
- Phone number, toll-free number, TTY number; and an
- E-mail link or contact form to the agency.

Search Engine

A search engine allows visitors to search online content. Public agency sites will have a site-specific search (to search the current Web site) and a *link to* Commonwealth search (to search all state agency sites).

WEB-R-24 **Public Search Engine Compatibility –** All public content posted on a Virginia government Web site shall be searchable and discoverable through public search engines.

WEB-R-25 **META Tags –** Every page on an Agency Web site shall contain an accurate Meta description in order to ensure any search engine can display meaningful search results.

WEB-R-26 **Periodic Search Testing –** All webmasters shall test search results relevant to their agency name and content internally and externally on a regular basis.

Internet Privacy Policy Statement

The Internet Privacy Policy Statement tells visitors how any collected personal information is handled on the site. It also contains other information about the site.

WEB-R-27 **Internet Privacy Policy and Statement –** To comply with Code of Virginia, § 2.2-3803 (B) at a minimum each agency shall:

- Develop an Internet privacy policy and an Internet privacy policy statement that explains the policy to the public; and,
- Tailor the policy and the statement to reflect the information practices of the individual agency.

WEB-R-28 **Internet Privacy Policy and Statement - Collection of Information –** To comply with Code of Virginia, § 2.2-3803 (B) at a minimum, the Internet Privacy Policy and Internet Privacy Policy Statement shall address:

- What information, including personally identifiable information, will be collected, if any;
- Whether any information will be automatically collected simply by accessing the website and, if so, what information;
- Whether the Web site automatically places a computer file, commonly referred to as a "cookie," on the Internet user's computer and, if so, for what purpose; and,
- How the collected information is being used or will be used.

Except for those systems listed in the Code of Virginia, § 2.2-3802, as exempt, the following also shall be included:

- A prescribed procedure for an individual to learn the purpose for which information has been recorded and particulars

about its use and dissemination; and
- A clearly prescribed and uncomplicated procedure for an individual to correct, erase or amend inaccurate, obsolete or irrelevant information.

WEB-R-29 **Internet Privacy Policy Statement**,- **Link Location** - A link to the Internet Privacy Policy Statement shall be featured in a conspicuous manner on the Web site home page, in the page footer.

WEB-R-30 **Internet Privacy Policy Statement – Data Retention –** The statement shall state that any personal information that is collected and retained is maintained in compliance with the Code of Virginia, §§ 2.2-3800 and 2.2-3803.

WEB-R-31 **Internet Privacy Policy Statement – Freedom of Information Act (FOIA)** – The statement shall remind users that information collected on this site may be provided to anyone that requests it under the "Virginia Freedom of Information Act."

WEB-R-32 **Internet Privacy Policy Related Requirements –** All agency Web sites shall have a Web Policy. The Web Policy shall include the following:

- Disclaimer – a statement that indemnifies the Commonwealth from responsibility for third party or externally linked content
- Link policy – a policy stating the criteria that allows a link to be placed on the site.
- FOIA – a statement that explains the agency's Freedom of Information Act policies and contacts.

Virginia Common Template - Site Design Considerations

This section addresses various considerations related to the design of an agency Web site, including site scalability and the use of fonts, frames, and style sheets.

Site Scalability

Site Scalability refers to the ability of the site to become narrower or wider depending on the visitor's browser's window width.

WEB-R-34 **Browser –** All template sites shall display and operate within most common browsers in a consistent manner.

Font Families

Font Families refers to the font types used to display text (Arial, Times Roman, etc.).

WEB-R-35 **Fonts**

- Menu and body type must use either serif or sans-serif typefaces. Script, ornamental display and black-letter typefaces are prohibited.
- All fonts used in a font-embedding solution must be properly licensed.

Frames

Frames refer to dividing the screen into areas each of which draws content from a separate file and has independent scrollbars.

WEB-R-36 **Frames –** The use of HTML frames is prohibited; however, the use of Inline Frames (IFRAMES) is permitted if the W3C recommendations (see: http://www.w3.org/TR/html4/present/frames.html#h) are fully compliant, which allows authors to insert a frame within a block of text.

Style Sheets

Style Sheets are Cascading Style Sheets (CSS files) used to control the appearance of Web pages.

WEB-R-37 **Style Sheets –** Agencies shall use style sheets to control the layout whenever possible. Tables shall not be used for layout unless they make sense when linearized.

Link Modification

Link Modification refers to the process of alerting the Virginia.gov portal of new, updated or outdated links to agency Web sites.

Each Agency's Webmaster is required to notify Virginia.gov of link changes. Due to the complexity of the Virginia.gov portal, it is critical that each Agency be held accountable for the content found on its individual Web sites. This Agency accountability is the only way the Commonwealth of Virginia can provide the public with the most current and accurate information.

Social Media

WEB-R-42 **Social Media** – The use of social media is an agency business decision. *For further details see the Social Media Topic Report at: http://www.vita.virginia.gov/oversight/default.aspx?id=365*

IT Accessibility

The *IT Accessibility Topic Report* (GOV103-02) is a complete rewrite of COV103-01 to align it with the U.S. Access Board's revised section 508 (accessibility) and inclusion of section 255 (telecommunications) pursuant to the *Code of Virginia*, § 2.2-2012

GOV103-02 replaces previous versions of this document. It incorporates the following topic- specific requirements by reference:

ITA-R-01 **Appendix A to Part 1194 – Section 508 of the Rehabilitation Act: Application and Scoping Requirements –** are incorporated by reference into the IT Accessibility Topic Report and are accessed at: https://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-ict-refresh/final-rule/text-of-the-standards-and-guidelines#appendix-a

Table of Contents

508. Chapter 1: Application and Administration
E101 General
E102 Referenced Standards
E103 Definitions

508 Chapter 2: Scoping Requirements
E201 Application
E202 General Exceptions
E203 Access to Functionality
E204 Functional Performance Criteria
E205 Electronic Content E206 Hardware
E207 Software
E208 Support Documentation and Services

ITA-R-02 **Appendix B to Part 1194 – Section 255 of the Communications Act: Application and Scoping Requirements**
- are incorporated by reference into the IT Accessibility Topic Report and are accessed at: https://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-ict-refresh/final-rule/text-of-the-standards-and-guidelines#appendix-b

Table of Contents

255. Chapter 1: Application and Administration
C101 General
C102 Referenced Standards
C103 Definitions

255. Chapter 2: Scoping Requirements
C201 Application
C202 Functional Performance Criteria C203
Electronic Content
C204 Hardware
C205 Software
C206 Support Documentation and Services

ITA-R-03 **Appendix C to Part 1194 – Functional Performance Criteria and Technical Requirements** – are incorporated by reference into the IT Accessibility Topic Report and are accessed at: https://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-ict-refresh/final-rule/text-of-the-standards-and-guidelines#appendix-c

Table of Contents

Chapter 3: Functional Performance Criteria
301 General
302 Functional Performance Criteria

Chapter 4: Hardware
401 General
402 Closed Functionality
403 Biometrics
404 Preservation of Information Provided for Accessibility
405 Privacy
406 Standard Connections

407 Operable Parts
408 Display Screens
409 Status Indicators
410 Color Coding
411 Audible Signals
412 ICT with Two-Way Communication
413 Closed Caption Processing Technologies
414 Audio Description Processing Technologies
415 User Controls for Captions and Audio Descriptions

Chapter 5: Software
501 General
502 Interoperability with Assistive Technology
503 Applications
504 Authoring Tools

Chapter 6: Support Documentation and Services
601 General
602 Support Documentation
603 Support Services

Chapter 7: Referenced Standards
701 General
702 Incorporation by Reference

Implementation Dates

The following requirement applies to information and communication technology (ICT) that is procured, developed, maintained, or used by Executive Branch agencies.

ITA-R-4: **Compliance Date** – Executive Branch agencies ICT covered by the *IT Accessibility Topic Report* (GOV103-01) are required to comply with the revised *IT Accessibility Topic Report* (GOV103-02) by January 18, 2018.

Existing ICT, including content, that meets the original GOV103-01 does not have to be upgraded to meet the revised requirements unless it is altered. This "safe harbor" clause (E202.2) applies to any non-altered component or portion of ICT that complies with GOV103-01 requirements. Any component or portion of existing, compliant ICT that is altered after the compliance date (January 18, 2018) must conform to the revised requirements in GOV103-02.

Existing requirements – prior to January 18, 2018, agencies must continue to comply with the existing GOV103-01 requirements.

Compliance with the **Section 255** guidelines is not required until the guidelines are adopted by the Federal Communication.

Legacy IT Solutions

Listed below are the requirements for Legacy IT Solutions (LIT):

LIT-R-01: **Agency Identification of Legacy IT solutions –** agencies must identify their legacy IT solutions and the *Prohibited* technologies they use to VITA by November 1, 2019.

LIT-R-02: **Legacy IT solutions –** agencies shall migrate off of all IT solutions that utilize *Prohibited* technology by January 1, 2024. Any intended use of legacy IT solutions beyond this date requires an approved Enterprise Architecture (EA) exception. Agencies shall submit these EA exception requests by January 1, 2020.

LIT-R-03: **Continued use of legacy technologies –** any intended use of *Prohibited* technologies requires an approved Enterprise Architecture (EA) exception. Agencies shall submit these EA exception requests by January 1, 2020.

LIT-R-04: **Agency business cases for legacy IT solution migration –** agencies shall develop business cases to determine the cost and impact of migrating their Legacy IT solutions to *Approved* technologies hosted on cloud-based platforms.

LIT-R-05: **Migration plan for IT solutions using *Prohibited* technologies –** agencies shall include a migration or replacement plan within their IT Strategic Plan for all Legacy IT solutions that do not have an approved EA exception.

LIT-R-06: **Add projects to agency IT Strategic Plans for *Prohibited* technologies –** agencies shall add CIO approved IBC (Investment Business Case) and IBC Addendum for projects and supporting BreTs to their agency IT Strategic Plans in support of the migration of their Legacy IT solutions do not have approved EA exceptions.

LIT-R-07: **Add procurements to agency IT Strategic Plans for *Prohibited technologies* –** agencies shall add any needed procurements to their agency IT Strategic Plan in support of the migration or replacement of their Legacy IT solutions that do not have approved EA exceptions.

Section 5.2 - ETA Database Domain

The Database Domain describes the technical components of the software systems that support storage and retrieval of data and the types of database software that will support applications. It includes the two topics of Database and Other Data Access Methods, and Data Management. Database and Other Data Access Methods addresses the components Hierarchical, Networked, Relational, and Object-oriented databases, and Other Data Access Methods. Data Management addresses the components Data Recovery and Backup, Data Dictionary, Database Administration, Enterprise Information Integration (EII), Database Design (Standards and Tools), and Data Modeling components.

Domain-wide Requirements

The following domain-wide requirements pertain to all topics and components in the Database Domain.

DB-R-01 Security, Confidentiality and Privacy Policies. Production databases shall be implemented in adherence with all security, confidentiality and privacy policies and applicable statutes.

DB-R-02 Support Tools Version/Release Levels. The version/release levels of all databases and related tools used to develop or support Commonwealth and/or agency "*mission critical applications"* shall have vendor or equivalent level support.

DB-R-03 Assess Business Recovery Requirements. An assessment of business recovery requirements is mandatory when acquiring, developing, enhancing or outsourcing database solutions. Based on that assessment, appropriate disaster recovery and business continuity planning, design and testing shall take place.

DB-R-04 Restrict Free-Form Data Entry/Update. Data entry and update to production databases using direct database access shall be restricted, logged and reported to business owners or other appropriate staff. Production database owners shall provide written delegated authority for this type of access.

Database and Other Data Access Methods

A database is a collection of information organized in such a way that a computer program can quickly select (access) desired pieces of data. A database management system (DBMS) is a software application providing management, administration, performance, and analysis tools for databases. The Database and Other Data Access Methods topic has Hierarchical, Networked, Relational, and Object-oriented (Object) components.

DB-R-05 Minimize DBMS Number/Version. Agencies shall minimize the number and versions of database management systems utilized.

DB-R-06 Support Connectivity. Newly deployed database technologies shall support Java Database Connectivity (JDBC) and Microsoft

connectivity technology (such as Open Database Connectivity (ODBC) or Object Linking and Embedding Database [OLEDB]).

Hierarchical Database

A hierarchical database is a kind of database management system that links records together in a tree data structure such that each record type has only one owner, e.g. an order is owned by only one customer. Hierarchical structures were widely used in the first mainframe database management systems. However, due to their restrictions, they often cannot be used to relate structures that exist in the real world. See DB-S-01 Table below for component standards.

Networked Database

A networked database is a database model conceived as a more flexible alternative to the hierarchical model. Where the hierarchical model structures data as a tree of records, with each record having one parent record and many children, the network model allows each record to have multiple parent and child records, forming a lattice structure. See DB-S-01 Table below for component standards.

Relational Database

A relational database is a database model in which the database is organized and accessed according to the relationships between data items without the need for any consideration of physical orientation and relationship. Relationships between data items are expressed by means of tables.

DB-R-07 **Relational DBMS for New Applications/Solutions.** A Relational DBMS shall be used as the "Database and Other Data Access Method" for newly developed or acquired applications/solutions.

DB-R-08 **Support Security Using Database Access Controls.** The SQL implementation and relational database products shall support database security using the following database access controls: GRANT and REVOKE privilege facilities, the VIEW definition capabilities, and some Discretionary Access Control (DAC) mechanisms.

Object-oriented (Object) Database

An object database (more correctly referred to as ODBMS or OODBMS for Object DBMS or Object Oriented DBMS, respectively) is a DBMS that stores objects as opposed to tuples (one row of a database table…one record) or records in a RDBMS (Relational Database Management System) or record-based DBMS. As data is stored as objects it can be interpreted only using the methods specified by its class. The relationship between similar objects is preserved (inheritance) as are references between objects. See DB-S-01 Table below for component standards.

Other Data Access Methods

Indexed Sequential Access Method (ISAM) is a common disk access method that stores data sequentially while maintaining an index of key fields to all the records in the file for direct access. The sequential order would be the one most commonly used for batch processing and printing (account number, name, etc.).

Virtual Storage Access Method (VSAM) is an IBM access method for storing data, widely used in IBM mainframes. It uses the B+tree method for organizing data.

See DB-S-01 Table below for component standards.

The following table provides strategic direction for agencies that are acquiring database and other data access method products.

Table DB-S-01: Database and Other Data Access Methods Technology Component Standard
(Updated April 04, 2011 to maintain compliance with DB-R-02)

Strategic:
Microsoft SQL Server: versions 2008 and 2005 Oracle: 11.X DB2: Version 9.x MySQL (shall have vendor or equivalent quality level support if used for *Mission Critical Applications*)
Emerging:
Object-oriented (Object) Databases Multidimensional Databases Real Time Databases
Transitional/Contained:
Microsoft SQL Server: Version 2000 – extended support ends 4/09/2013 Oracle: Version 10.1 – extended support ends 1/2012 Version 10.2 – extended support ends 7/31/2013 DB2: Version 8.1 with special extended support (until 9/08/2012) IMS VSAM Adabas MAPPER, BIS, Cool Ice
Obsolescent/Rejected:
All versions/release levels of Database and Other Data Access Methods that do not have vendor or equivalent level quality support Desktop database products (Such as Microsoft Access, Lotus Approach, or Paradox, are considered desktop productivity tools. ***They shall not be used for multi-user applications***.) All Networked Databases All Hierarchical Databases not categorized as "Transitional/Contained" All other non-specified Database and Other Data Access Methods *Notes:* • *Oracle version 9.2 extended support ended 7/2010* • *DB2 version 8.1 support ended on 9/08/2009 – additional paid for support is available until 9/08/2012*

Exception History: *02/12/2009: CIO approved adding the MS SQL 2008 DBMS product as a strategic technology*

Data Management

Data Management defines the set of capabilities that support the usage, processing and general administration of unstructured information. The Data Management topic has Data Recovery and Backup, Data Dictionary, Database Administration, Enterprise Information Integration (EII), Database Design (Standards and Tools), and Data Modeling components. Other than the Domain-wide requirements identified above, no specific requirements are identified for the Database Design (Standards and Tools) component.

Data Recovery and Backup

Data Recovery and Backup defines the set of capabilities that support the restoration and stabilization of data sets to a consistent, desired state.

DB-R-09 **Test Production Databases.** Production databases shall be periodically tested for recoverability according to requirements for their use and preservation.

DB-R-10 **Business/Recovery Strategies Shall Address Business Requirements.** All backup and recovery strategies shall address the business requirements of the data regarding availability, accuracy, and timeliness of data.

DB-R-11 **Backup Metadata.** Metadata (database schemas, structures, data definitions, etc.) shall be backed up along with the data.

DB-R-12 **Recover to Point-In-Time and Point-Of-Failure.** Production databases supporting mission critical applications shall be recoverable to a point-in-time and point-of-failure.

DB-R-13 **Define High Availability Strategy.** Databases requiring 24 x 7 availability shall have a high availability strategy such as failover, mirroring, and/or the use of online backups.

DB-R-14 **Production Databases.** Production databases shall be on different physical machines than the test and development databases.

Data Dictionary

A Data Dictionary is a database about data and databases. It holds the name, type, range of values, source, and authorization for access for each data element in the organization's files and databases. It also indicates which application programs use that data so that when a change in a data structure is contemplated, a list of affected programs can be generated. The data dictionary may be a stand-alone system or an integral part of the DBMS.

DB-R-15 **Implement a Data Dictionary.** A Data Dictionary is required for any development that results in new databases and any enhancement activities that result in new tables being added to existing databases.

Database Administration

Database administration is the process of establishing computerized databases and insuring their recoverability, integrity, security, availability, reliability, and performance.

DB-R-16 **Assign DBA (Database Administrator) Responsibilities.** Agencies shall formally assign the responsibilities for database administration.

DB-R-17 **Limit DBA Permissions.** Database permissions shall be granted at the minimum level required. Limit the members of the System or Database Administrators role to trusted DBAs. Create custom database roles, if required, for better control over permissions. Business data manipulation by DBAs shall not be permitted.

DB-R-18 **Control Application Access and Passwords. Reset Default Access.** Production application programs or interfaces shall never be given System or Database Administration authority. Default accounts shall be changed. Production passwords shall be changed from test and development environments.

DB-R-19 **Limit Query/Reporting Database Access to Read-Only.** Direct production database access for ad-hoc queries and end-user reporting shall be read-only.

DB-R-20 **Evaluate and Apply Patches.** DBAs shall evaluate the latest service packs and security patches released by DBMS vendors. When the DBMS is utilized by a 3rd party application, all patches shall be certified by that application vendor before being applied. Security patches shall be applied and the other service packs and patches should be applied according to DBMS and related 3rd party application vendor recommendations as needed.

DB-R-21 **Monitor Databases for Planning and Availability.** Databases for mission critical applications shall be monitored proactively for capacity planning purposes and to maintain high availability.

Enterprise Information Integration (EII)

EII is the industry acronym for **Enterprise Information Integration**. It describes the process of using data abstraction to address the data access challenges associated with data heterogeneity and data contextualization. Data is the foundation upon which the "Information Age" and critical components such as the burgeoning Web 2.0 and a future Semantic Web are being built. Uniform data access and uniform information representation are critical aspects of this journey.

An EII product offers virtualization of heterogeneous data where data takes the form of SQL, Extensible Markup Language (XML), Data-returning Web services, and other Universal Resource Identifier (URI) resources that may be referenced. Such SQL data is typically accessible via Open Database Connectivity (ODBC, Java Database Connectivity (JDBC), Active X Data Objects (ADO.NET), Object Linking and Embedding Database (OLEDB) APIs. XML is generally URI based, and is thus accessible via (Web-based Distributed Authoring and Versioning) WebDAV.

EII products enable loose coupling between homogenous-data consuming client applications and services and heterogeneous-data stores. Such client applications and services include desktop productivity tools (spreadsheets, word processors, presentation software, etc.), development environments and frameworks (J2EE, .NET, Mono, Simple Object Access Protocol [SOAP] or RESTian [Representational State Transfer] web services, etc.), Business Intelligence (BI), Business Activity Monitoring (BAM), Enterprise Resource Planning (ERP), Customer Relationship Management (CRM), Business Process Management (BPM) and/or Business Process Execution Language (BPEL), and Web Content Management.

DB-R-22 **Enterprise Information Integration (EII) Tool.** Agencies (excluding institutions of higher education) shall not purchase an EII tool without VITA approval.

Data Modeling

Using modeling tools to describe (usually graphically) the attributes and tables (fields and records) of the organization of a database; it is often created as an entity relationship diagram. In many tools, the SQL code that defines the data structure (schema) in the database is automatically created from the visual representation.

DB-R-23 **Implement a Data Modeling Tool.** Agencies shall select and implement a consistent data modeling tool.

Section 5.3 - ETA Information Domain

The Information Domain assists business and technical leaders in making sound decisions related to data warehouse design and acquisition of data warehouse, business intelligence, and other reporting tools and products. This domain also provides a framework for defining responsibility for data integrity and distribution. An effective Information Domain will enable the Commonwealth to leverage the most value from its data assets. This domain addresses the Enterprise Business Intelligence (EBI) Suite, Other Reporting, Data Management, Business Intelligence, Knowledge Management, Electronic Records Management, and Health Information Exchange topics.

Domain-wide Requirements

The following domain-wide requirement pertains to all topics and components in the Information Domain.

INF-R-17 **Production Data –** Agencies shall ensure that all dynamic production data (i.e. Data-at-Rest) is stored on production servers (including Storage Area Networks and Network Attached Storage units). Local storage may be used for the temporary storage of transactional data (i.e. Data–in-Motion). Local storage may also be used for static production data (i.e. GIS), but the data must be stored in multiple locations or have proper backup copies. Peer-to-peer networks are not to be used for sharing any production data.

Enterprise Business Intelligence (EBI) Suite

The EBI topic includes the components: Ad Hoc End-User Reporting, Standardized/Canned Reporting, and Online Analytical Processing (OLAP). As of this time, no specific requirements have been identified for the Standardized/Canned Reporting component.

The technology component standard table below provides strategic technology directions for agencies that are acquiring reporting software systems to be used either as stand–alone systems or as subsystems of larger applications.

Table INF-S-01: **Reporting (for agencies that do not already support another solution) Technology Component Standard** *New: 04/04/2011*
Strategic:

• Ad–hoc End User, Standardized/Canned
  ○ LogiXML
• OLAP
  ○ LogiXML
  ○ Microsoft SQL Server Reporting Services, Analysis Services
  ○ Oracle BIEE OLAP Reporting

Emerging:
Transitional/Contained:
• Oracle (Hyperion) Brio
Obsolescent/Rejected:
• R&R Report Writer (Plan–Be, formerly Concentric)

Ad Hoc End-User Reporting

Ad hoc query provides the business analyst with the ability to pose specific questions to produce a result without needing the programming of a report by IT. The ad hoc nature of these queries implies a short shelf life where some situation is being researched or a new opportunity is being explored.

Following are requirements that all newly acquired Information/Business Intelligence ad-hoc reporting software tools must support.

INF-R-05 **Ability to share queries –** All newly acquired Information/ Business Intelligence ad hoc end-user tools shall be able to share an ad hoc query with others. This enables the reuse and efficient utilization of agency resources.

INF-R-06 **Intuitive interface –** All newly acquired Information/Business Intelligence ad hoc end-user tools used to build a report shall have an intuitive interface, with "point and click" features for adding elements, filtering data, and sorting the results, with no programming knowledge required.

Online Analytical Processing (OLAP)

OLAP tools view information in the form of cubes, or multiple dimensions and allow the user to drill down to lower levels of detail, and slice across different dimensions such as time or commodity. These tools are generally used by the business analyst in conducting research to answer business questions as part of the decision making process.

Following are requirements that all newly acquired Information/Business Intelligence OLAP software tools must support.

INF-R-07 **Drill-down capability –** OLAP tools shall have the ability to drill into the details of a cell in an OLAP cube by going to the source database.

INF-R-08 **OLAP Export –** OLAP tools shall have the ability to export the results to a standard spreadsheet format such as .csv or .xls.

INF-R-09 **Easy cube manipulation –** The interface to manipulate data in the cube shall have "point and click" and "drag and drop" features for analyzing the available data.

Other Reporting

The Other Reporting topic includes the components: Query, Precision/Recall, Ranking, Classification, and Pattern Matching. As of this time, no specific requirements have been identified for this topic.

Data Management

The *Data Management* topic is concerned with the components that affect the quality, management, meta-management, accessibility, and recovery of electronic data resources.

Requirements have been identified within the *Data Management* topic for the Data Standards and Data Classification (security and access) components.

Data Standards

It is important to address the issues of data and data quality through the use of data standards. Data standards are important in the quest for data integration and consist of a framework used to classify or define data. These standards may include Data Element Naming, Database Object Naming, Metadata Requirements, Data Modeling, and Geo-Spatial Requirements.

Following are requirements that all newly acquired Information/Business Intelligence software tools must support.

INF-R-10 **Standard file formats –** Agencies shall ensure that all software tools or packages that create files or data stores do so in a format that is based on an underlying open or de facto standard or provides the capability to export to such a format.

Data Classification (security and access)

Data must be classified according to its degree of sensitivity in a universally understandable manner. The degree of sensitivity can be determined by applying the appropriate State, Local or Federal laws or regulations to the data. Sensitivity levels are determined by the type of information that is in an automated system. The information that has the least amount of sensitivity might include things such as summary revenue and expense data for the Commonwealth. Data that is made generally available without specific custodian approval and that has not been explicitly and authoritatively classified as confidential is not considered sensitive. Highly sensitive information would include information that must be protected to meet state and federal Privacy Act requirements including data such as social security numbers, credit card numbers, criminal and medical histories, etc. It is also data whose loss, corruption, or unauthorized disclosure would be a violation of state and federal statues, mandates and regulations. The term "in a universally understandable manner" implies there should be standard definitions for the different sensitivity classifications. In addition, the data needs to maintain its security classification as it traverses any physical or logical boundary such as an agency, computer-related device, network, or software application system.

INF-R-11 **Sensitivity classification –** Data that is sensitive shall be classified by the agency according to its degree of sensitivity in a universally understandable manner.

INF-R-12 **Security classification –** Data that requires a security classification shall maintain its security classification as it traverses any physical or logical boundary such as an agency, computer- related device, network, or software application system.

Business Intelligence

Business intelligence (BI) is a broad category of application programs and technologies for gathering, storing, analyzing, and providing access to data to help enterprise users make better business decisions.

Requirements have been identified within the *Business Intelligence* topic for the Data Warehouse/ Data Marts component. Other than the Information Domain-wide requirements identified above, no specific requirements are identified for the other Business Intelligence components: Operational Data Stores, Extraction, Transformation and Loading (ETL), Data Storage Structures, Data Mining, Demand Forecasting and Management, Balanced Scorecard, Decision Support and Planning, Business Analytics Suites, and Dashboards.

The phrase business intelligence (BI) may refer to

1) a set of business processes,
2) the technology used in these processes, or
3) the information obtained from these processes.

Data Warehouse / Data Marts

A data warehouse is a database designed to support decision-making in an organization or enterprise. It is refreshed, or batch updated, and can contain massive amounts of data. When the database is organized for one department or function, it is often called a "data mart" rather than a data warehouse. The data in a data warehouse is typically historical and static in nature.

INF-R-13 **Read-only Data Warehouse –** Access shall be restricted to read- only for end users of the data warehouse.

INF-R-14 **Database Standard –** Data warehouses and data marts that use relational databases shall conform to all of the Requirements and Technology Product Standards for databases as defined above in Section 2: ETA Database Domain.

To ensure that data warehouse and data mart implementations are built to meet the current and future business needs of an agency, executive sponsorship and representation by the business community on the project is required. Without this leadership, business intelligence (BI) projects run the risk of not providing the anticipated rewards or even failing altogether.

INF-R-15 **Business community representation –** A representative of the business community shall be involved in the entire development life cycle of all BI projects.

INF-R-16 **Executive sponsorship –** Project sponsorship shall be obtained from one or more executives within the upper management of the related organization prior to initiating any Data Mart or Data Warehouse project.

The technology component standard table below provides strategic technology directions for agencies that are acquiring business intelligence software systems to be used either as stand–alone systems or as subsystems of larger applications.

Table INF-S-02: Business Intelligence (for agencies that do not already support another solution) Technology Component Standard *NEW: 04/04/2011*
Strategic:

• All business intelligence areas
  o LogiXML
• Extract, Transform and Load
  o LogiXML
  o Microsoft SQL Server Integration Services
• Business Analytics, Decision Support
  o LogiXML
  o Microsoft SQL Server Analysis Services
  o Statistical Analysis System (SAS)
  o SPSS

Emerging:
Transitional/Contained:
• DB2 UDB reporting
Obsolescent/Rejected:
• R&R Report Writer (Plan–Be, formerly Concentric)

Electronic Records Management

The Commonwealth's Electronic Records Management (ERM) Topic provides guidance and direction to public entities to address the unique requirements for those public records that are electronic in form. ERM is designed to assist agencies to identify and manage electronic records effectively and efficiently through the establishment of an appropriate set of records management controls. ERM provides a proactive framework to manage electronic records through their life cycle. It starts at the initial development stage of an automated application and continues through the retirement of any associated electronic records.

The following are Electronic Records Management topic-wide requirements:

ERM-R-01 **Develop IT Systems with ERM Capability –** When an agency builds a new automated system or significantly updates an existing automated system, the agency shall ensure that the system has the ability to manage records by their appropriate State Agency Records Retention & Disposition Schedules

ERM-R-02 **ERM Training and Awareness –** Agencies shall require training and education programs for all aspects of electronic records management to be an integral and ongoing component of an agency records management program.

ERM-R-03 **External Service Providers –** Agencies shall ensure that all contracts related to external providers hosting applications that contain Commonwealth identified public records have appropriate terms and

conditions that require the vendor to manage those electronic records in compliance with the agency approved records retention and disposition schedule.

ERM-R-04 **Timely Disposition for Electronic Records –** Agencies shall establish, maintain and implement procedures to ensure all public electronic records are retained until no longer needed and disposed of in accordance with their corresponding approved LVA retention and disposition schedule.

ERM-R-05 **Accessibility During the Life cycle of Electronic Records –** Agencies shall take appropriate measures to ensure electronic records are accessible for as long as required by their approved records retention and disposition schedule. Measures could include but are not limited to maintaining the hardware, software and media necessary to access the records; maintaining the pertinent technical expertise, manuals and documentation required to use this hardware, software, and media in order to access the records; refreshing electronic storage media; or converting those records to a different format that makes the records accessible.

ERM-R-06 **Replacement or Upgrading of Legacy Systems –** When existing systems are replaced or upgraded, agencies shall ensure electronic records stored in the old system are either:

i. maintained and managed in the old system until appropriately disposed according to their applicable retention and disposition schedules; or
ii. migrated and managed in the new system until appropriately disposed according to their applicable retention and disposition schedules.

Life Cycle Phases of Electronic Records – Create Phase

The create phase begins at the point in time when a public record is first created in an electronic format and stored in an automated system. Requirements related to the create phase include the following:

ERM-R-07 **Electronic Records' Metadata –** Each electronic record created shall have metadata sufficient to manage the record throughout its life cycle. Types of metadata must include, but are not limited to, the following:

i. "Descriptive" metadata allows for basic identification of a record through title, author, and keywords.
ii. "Structural" metadata indicates how objects are put together, for example, how pages are ordered to form chapters.
iii. "Administrative" metadata includes technical information to help manage a document, such as file type, creation date, format, and access restrictions.

Life Cycle Phases of Electronic Records – Access Phase

The access phase begins after a public record is initially created and stored in an electronic format. Access is defined as the right bestowed by law to access public records and includes the opportunity and means of finding, using, or retrieving information from public records stored in electronic formats. There are no requirements for this phase.

Life Cycle Phases of Electronic Records – Maintain Phase

The maintain phase includes the maintenance in an unaltered form of an electronic record together with its metadata. The requirement related to the maintain phase is:

ERM-R-08 **Disaster Preparedness Plan –** Agencies shall maintain an adequate electronic records disaster preparedness plan for the protection of agency electronic records and to assist in the recovery of agency electronic records from a disaster.

Life Cycle Phases of Electronic Records – Store Phase

The store phase occurs after an electronic record is no longer needed to support current business practices and prior to that record completing its LVA established retention period. During this period of time, the electronic record must be safely stored until such time that it can be properly disposed of. In this phase, an electronic record may be inactive or semi- active and used to support other activities such as research. The requirement related to the store phase is:

ERM-R-09 **Safekeeping Electronic Records in Storage –** Agencies shall store electronic records no longer needed to support current business practices but that have not satisfied their LVA established retention criteria by:

i. ensuring the same level of safekeeping as when the electronic records were first created and used to actively support agency business needs;
ii. ensuring that those electronic records can continue to be accessed electronically through hardware, software, and media migrations and upgrades; and
iii. ensuring the pertinent manuals and documentation required to use this hardware, software, and media in order to access the records are maintained.

Life Cycle Phases of Electronic Records – Dispose Phase

The dispose phase addresses an electronic records final disposition; either destruction or permanent retention through archiving. Permanent retention of electronic records through archiving can be handled by the agency or through transfer of the records to the Archives at the Library of Virginia. Destruction of electronic records must be accomplished in accordance with LVA retention and disposition schedules and in a manner that permanently eliminates or deletes the electronic records, beyond any possible reconstruction. The requirement related to the dispose phase is:

ERM-R-10 **Disposition of Electronic Records –** Agencies shall develop and implement procedures to ensure electronic records are disposed of in a timely fashion as scheduled by their retention and disposition schedules.

ERM-R-11 **Identify Electronic Records Subject to Legal Hold –** Agencies shall identify all records custodians (staff and/or vendors) that might have electronic records subject to a litigation hold and ensure that the custodians are aware of their preservation responsibilities.

ERM-R-12 **Legal Hold –** Agencies shall develop and implement procedures to ensure all electronic records identified and documented as related to a specific legal hold event be preserved and protected. This includes ensuring that those records will not be destroyed or reformatted until the event resulting in the records legal hold has concluded and all appeal periods are exhausted even if the duration exceeds the relevant records retention and disposition schedule.

Health Information Exchange

The Commonwealth of Virginia, led by the Health IT Advisory Commission and under the technical infrastructure guidance of the Health IT Standards Advisory Committee (HITSAC) has developed a plan to implement a state wide health information exchange (HIE). The audience for this topic report includes business and technical leaders in state and local agencies that will connect to the National Health Information Network (NHIN) through the state HIE.

The standards presented in the report are the first set of technical infrastructure domain requirements for the Commonwealth of Virginia Health Information Exchange (COV-HIE). The COV-HIE is a network and a service, and "exchange" within its name is both a noun and a verb. As a noun, it is a digital network allowing providers to exchange electronically and with semantic interoperability health care data about patients, they share. As a verb, it is a collection of services that reliably communicate clinical data between providers by identifying patients and locating their digital medical records across various electronic medical record systems.

The following are HITSAC's initial architectural requirements for the COV-HIE. State agencies, within the Executive Branch, shall comply with these requirements in connecting to the COV-HIE. The current requirements are organized into four sub-topic areas:

1. Interoperability
2. Technical Infrastructure
3. Data
4. Privacy and Security

COV-HIE Architecture - Interoperability Sub-Topic

Interoperability is defined by ONC as the ability of health information systems to work together within and across organizational boundaries in order to advance the effective delivery of health care for individuals and communities. The requirements for interoperability are as follows:

HIE-R-01 **Office of the National Coordinator standards –** the COV-HIE shall be congruent with the standards established by the Office of the National Coordinator (ONC) and be routinely certified by ONC.

HIE-R-02 **HITSP Interoperability Specifications and Capabilities –** the COV- HIE shall implement the HITSP Interoperability Specifications and Capabilities. The COV-HIE shall support the ONC interoperability and data exchange functions of "meaningful use" of Electronic Health Records (EHR).

HIE-R-03 **HIE data exchanges –** all HIEs within the Commonwealth that exchange data in electronic form with state agencies shall comply with the HITSP Interoperability Specifications and Capabilities.

HIE-R-04 **Electronic eligibility and claims transactions –** the COV-HIE shall support electronic eligibility and claims transactions: adherence to HITSP Capability 140 (communicate benefits and eligibility) and HIPAA standards.

HIE-R-05 **Electronic prescribing and refill requests –** the COV-HIE shall support electronic prescribing and refill requests: utilize an established eprescribing vendor to adhere to HITSP Capabilities 117 and 118 (prescription).

HIE-R-06 **Prescription fill status and/or medication fill history –** the COV-HIE shall support prescription fill status and/or medication fill history: adherence to HITSP Capabilities 117 and 118.

HIE-R-07 **Clinical summary exchange –** the COV-HIE shall support clinical summary exchange for care coordination and patient engagement: adherence to HITSP Capabilities 119 and 120 as the basis for interoperability of patient documentation (structured and unstructured).

HIE-R-08 **Quality reporting –** the COV-HIE shall support quality reporting: adherence to HITSP Capability 130.

HIE-R-09 **Electronic public health reporting –** reporting the COV-HIE shall support electronic public health reporting: adherence to Interoperability Specification 11.

HIE-R-10 **Electronic clinical laboratory ordering and results –** the COV-HIE shall support electronic clinical laboratory ordering and results delivery: adherence to HITSP Capabilities 126 and 127.

HIE-R-11 **Patient identification –** the COV-HIE shall adopt the HITSP Capabilities for patient *identification when issued.*

COV-HIE Architecture – Technical Infrastructure Sub-Topic

The requirements for technical issues are as follows:

HIE-R-12 **Data exchange functions –** The COV-HIE shall support the data exchange functions for achieving meaningful use of certified Electronic Health Records (EHR) technologies.

HIE-R-13 **NHIN connectivity requirements –** the COV-HIE shall support the connectivity requirements of the National Health Information Network (NHIN) and provide connectivity to the NHIN for providers and HIEs in the Commonwealth of Virginia.

HIE-R-14 **NHIN connection –** the COV-HIE shall provide a connection to the NHIN.

HIE-R-15 **Services –** the COV-HIE shall provide Security Services, Patient Locator Services, Data/Document Locator Services, and Terminology Services as defined by HITSP Interoperability documents.

HIE-R-16 **"Hybrid" logical architecture –** providers of health care services shall maintain the patient clinical data for the COV-HIE on edge (staging) servers that are separate from, and updated regularly by, the providers' electronic medical record transaction systems. This requirement describes the "hybrid" logical architecture.

HIE-R-17 **Daily data synchronization –** implemented solutions shall provide data synchronization from provider systems daily.

HIE-R-18 **24 by 7 service levels –** the COV-HIE shall provide high availability with redundancy and fail-over to achieve 24 by 7 service levels.

COV-HIE Architecture – Data Sub-Topic

The requirements for the management of data are as follows:

HIE-R-19 **ONC structured or unstructured data formats –** the COV-HIE will communicate with edge servers to provide data in structured or unstructured data formats as defined by ONC. Even though the federal government recognizes storing data in the Continuity of Care Document (CCD) and Continuity of Care Record (CCR) formats, the COV-HIE shall only require the data in the CCD format to ease the burden on the organizations generating the data to share.

HIE-R-20 **Data storage –** the COV-HIE shall follow the ONC specifications for data storage.

HIE-R-21 ***Coded health care terminologies –*** *the COV-HIE shall adhere to the set of coded health care terminologies defined by the Federal Health Architecture (FHA).*

COV-HIE Architecture – Privacy and Security Sub-Topic

The requirements for privacy and security are as follows:

HIE-R-22 **ARRA privacy and security provisions –** the COV-HIE shall incorporate ARRA privacy and security provisions related to security breach restrictions and disclosures, sales of health information, consumer access, business associate obligations and agreements.

HIE-R-23 **HIPAA Privacy Rule –** the COV-HIE shall incorporate Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule for permitted uses and disclosures and individual rights related to protected health information.

HIE-R-24 **HIPAA Security Rule –** the COV-HIE shall incorporate Health Insurance Portability and Accountability Act (HIPAA) Security Rule for administrative, technical, and physical security procedures.

HIE-R-25 **Confidentiality of Alcohol and Drug Abuse Patient Records Regulations –** the COV-HIE shall incorporate Confidentiality of Alcohol and Drug Abuse Patient Records Regulations for substance abuse treatment programs.

HIE-R-26 **HHS Privacy and Security Framework –** the COV-HIE shall incorporate Health and Human Services (HHS) Privacy and Security Framework for a single consistent approach to address the privacy and security challenges related to electronic health information exchange.

HIE-R-27 **Federal requirements for protection of health data –** the COV-HIE shall incorporate federal requirements for protection of health data for federal health care delivery organizations such as the Department of Veterans Affairs and the Department of Defense.

HIE-R-28 **ONC specifications for privacy and security –** the COV-HIE shall adopt the ONC specifications for privacy and security when issued.

HIE-R-29 **Security certificate –** the COV-HIE shall (as part of the onboarding process) issue a security certificate to the trusted entity.

Section 5.4 - ETA Integration Domain

Integration Domain defines the functions that enable communications in a distributed system and defines the tools that improve the overall usability of an existing architecture made up of products from many different vendors on multiple platforms. Integration tools and products allow organizations to share data between disparate systems that do not communicate easily. Integration tools and products have been described as the software "glue" that allows distributed, multi-tiered applications to work in a world of global networks.

The ETA Integration Domain consists of the following topics: Database Integration, Message Integration, Transaction Process Monitor Integration and Services, Application Integration Middleware and Services, Enterprise Service Bus, Service-Oriented Architecture, Instant Messaging and Mashup.

Domain-wide Requirements

The following domain-wide requirements pertain to all topics and components in the Integration Domain.

INT-R-01 **Security, Confidentiality, Privacy and Statutes.** Agencies shall implement integration applications/ solutions in adherence with all security, confidentiality and privacy policies and applicable statutes.

INT-R-02 **Software Tools Version/Release Support.** The version/release levels of all integration software tools shall have vendor or equivalent quality level support available.

INT-R-03 **Planning.** Before acquiring a central integration solution, agencies shall map their present integration sources and uses, and shall develop a plan in consultation with the Virginia Information Technologies Agency (VITA) Integration Competency Center (ICC) for migration to the central integration solution.

INT-R-04 **Integration Solutions.** Agencies shall use integration solutions that are scalable, extensible, and maintainable.

INT-R-05 **Defined Interfaces.** Agencies shall carefully define their interfaces and interface business requirements.

INT-R-06 **Testing Integration Modifications.** Integration tools and services shall be thoroughly tested. Consideration shall be given to the need to maintain a separate environment for testing modifications.

INT-R-07 **Shared Resource.** Before acquiring integration solutions, agencies shall contact the VITA ICC to determine if similar integration solutions exist that could be a shared resource across several agencies. To reach the VITA ICC, contact the VITA Customer Care Center (VCCC) by phone 1-866-637-8482, or 804-786-3932 in

Richmond, or by Email: vccc@vita.virginia.gov or go online: http://www.vita.virginia.gov/vccc/incident/vcccincident.cfm

Database Integration

Database tools and products enable applications to communicate with one or more local or remote databases. They do not transfer calls or objects. For example, database integration does not allow for two-way communication between servers and clients. Servers cannot initiate contact with clients, they can only respond when asked. The discussion of database integration is broken into Directory Services, Metadata, Access Services, and related guidance. Guidance information may direct the reader to other domains once they become available.

Directory Services

A directory may be described as a specialized database of lists. Directories serve a wide variety of functions in a computing environment and are used by applications including email, security, and naming services. Directory services are important as tools in the communications process and a decision about directory services is one of the most important foundational decisions an agency can make in planning a distributed architecture and integration strategy. Having a directory strategy is an integral part of promoting interoperability and, location transparency, and lowing future maintenance costs in a distributed environment.

Directory Services Requirements:

INT-R-08 Directory Services. Agencies shall employ Lightweight Directory Access Protocol (LDAP)-compliant directory services. This lays the groundwork for uniform decentralized lists that can be aggregated centrally for use by the Commonwealth.

Table INT-S-01: Directory Services Technology Component Standard *Reviewed 10-1-2008*
Strategic:
LDAP, DNS & GDS Sun JDAP; MS Active Directory (ADSI)
Emerging:
None
Transitional/Contained:
X.500 DAP
Obsolescent/Rejected:
Novell NDS

Database Metadata Services

Database metadata services are repositories of data about data. The purpose of the metadata repository is to provide a consistent and reliable means of access to data. The repository itself may be stored in a physical location or may be a virtual database, in which metadata is drawn from separate sources. Metadata may include information about how to access specific data, or more detail about it, among a myriad of possibilities.

Technology Component Standard INT-S-02 provides technology ratings for database metadata services. In general, the technologies listed as strategic are based on open standards.

Table INT-S-02: Database Metadata Services Technology Component Standard *Reviewed 10-1-2008*
Strategic:
OMG's UML, MOF MDC's XMI (XML, DTD, Schema) OIM's exchange format XIF (XML) Accessible, computer aided metadata documentation (e.g., ERwin modeling tool) and a metadata repository
Emerging:
Active metadata repository
Transitional/Contained:
Configurable metadata separate from application but proprietary to system.
Obsolescent/Rejected:
Business rules and meaning hard coded into applications. Hard copy only documentation of metadata.

Database Access Services

Database access services refer to software applications that are designed to arrange and store data for ease and speed of search and retrieval.

Table INT-S-03: Database Access Services Technology Component Standard *Reviewed 10-1-2008*
Strategic:
DB Adapters or Drivers: ODBC, JDBC, xDBC, OLE-DB (platform specific) XML point to point contracts (e.g., for Schemas) ODBC/SQL compliant gateways XML messaging
Emerging:
None
Transitional/Contained:
OLE (replaced) Screen Scrapers as a mainframe access Non-ODBC/SQL compliant Gateways Translators for non-standard SQL, XML, etc.
Obsolescent/Rejected:
None

Message Integration

Message-Oriented Middleware also known as Message Brokers, MOM, and Messaging Broker, provides an interface between applications or application parts, allowing for the transmission of data back and forth intermittently. Messaging middleware is similar to an e- mail system that transfers messages between people, except that it sends information between applications. MOM is typically asynchronous and peer-to-peer, but most implementations support synchronous message passing as well. In general, a message- oriented middleware has one of two architectures: the hub-and-spoke model or the network-centric bus model, also called the message-bus model. If the destination

application is not available because of connection failure or because the application is busy, the middleware stores the data in a message queue until the application becomes available.

Message Formats

In this section, the term "messages" will be used in the broadest sense to encompass transaction-based messages as well as entire file transfers. To many messaging systems, the format of the content of the message doesn't matter as long as it has the understood envelope/wrapper or an operating system recognizable format. However, the format of the content is very important to the receiving operating system, application, or user. Format translations may be performed by integration products. Also included in this section are messages that are object-oriented. These messages are requests or replies that are issued or received by applications or databases.

Table INT-S-04: Message Formats **Technology Component Standard** *Reviewed 10-1-2008*
Strategic:
XML and CSS (presentation style configurable by administrator for device types) 7 bit ASCII; 8 bit ASCII; EBCDIC (translation)
Emerging:
None
Transitional/Contained:
None
Obsolescent/Rejected:
None

Message Transfers

Message transfers refer to software applications that are designed to provide for correct and reliable end-to-end data transport between communication partners.

Table INT-S-05: Message Transfers **Technology Component Standard** *Reviewed 10-1-2008*
Strategic:
File and Data Requests/Replies FTP XML file transfer Presentation and Translation Services for Security Encryption/Decryption Services (A wide variety of encryption algorithms are strategic depending on security needs) e.g., Symmetric Encryption, DES, Triple DES, RC2, RC4 Terminal Emulation APPC LU6.2
Emerging:
None
Transitional/Contained:
Presentation and Translation Services for Security Proprietary style layout separate from application Terminal Emulation SNA/SDLC (OSI level 2)
Obsolescent/Rejected:
FTP whenever security required

Messaging Integration

The recommended messaging protocols also know as email (electronic mail) protocols apply to mail messaging and/or other application-to-application messaging. Email is the exchange of computer-stored messages by telecommunication. Mail programs should support use of MIME (Multipurpose Internet Mail Extensions), be SMTP/ESMTP enabled (Simple Mail Transfer Protocol/Extended Simple Mail Transfer Protocol), and provide proxy through IMAP4/POP3 servers (Internet Message Access Protocol 4/Point of Presence 3). Mail programs that interface with Windows clients use Microsoft's MAPI (Messaging Application Programming Interface) interface. Middleware protocols used by mail applications and/or other applications include: LDAP, DNS (Domain Name System), SSL (Secure Sockets Layer), and additional security protocols.

Message Integration requirements

INT-R-09 **Email Protocols.** Agency email messaging shall be SMTP and MIME compatible. Local governments are encouraged to follow this standard as well.

INT-R-10 **Emails.** The Message Transfer Agent (MTA) in email applications should be LDAP enabled.

Table INT-S-06: Message Integration **Technology Component Standard** *Updated 10-1-2008*
Strategic:
IMAP MAPI SMTP/MIME XSL (presentation style and content configurable by user)
Emerging:
XSL (presentation style and content configurable by user)
Transitional/Contained:
X.400 POP3 VIM CMC
Obsolescent/Rejected:
Non-Internet compatible email

Transaction Process Monitor Integration and Services

Distributed transaction processing ensures transaction integrity for transactions that involve databases. Transaction processing is the independent execution of a set of operations on data in a relational database, which treats that set of actions as a single event. If any part of the transaction process fails, the entire transaction fails and all participating resources are rolled back to their previous state.

Transaction processing monitors and some web services software are critical to the 3-tier application client/server computing model because they facilitate writing of the programs that track transactions across multiple platforms. In the n-tier world, the application layer functions between the presentation layer on the PC and the data layer on the mainframe, Unix, or Windows-based systems. Historically some of the following services have been

included in transaction processing monitor middleware: two-phase commits, failure/recovery, synchronization, scheduling, repeat attempts, business-rule-based transaction workflow services, message queuing resource managers, and load balancing. Perhaps the most significant feature of the TP monitor is its ability to funnel database requests.

Technology Component Standard INT-S-07 provides strategic open protocols and examples of mainframe programs used to define the typical work performed by transaction processing monitors. In general, those technologies listed as strategic are based on open standards.

Table INT-S-07: Transaction Process Monitor Integration and Services Technology Component Standard *Updated 10-1-2008*
Strategic:
SOAP WSDL HTTP M-POST
Emerging:
None
Transitional/Contained:
X/Open: XA interface (X/Open is the standard, XA is the interface) STDL (structured transaction definition language) DTP (distributed transaction processing) CPI-C (common program interface for communications) CORBA DCOM
Obsolescent/Rejected:
None
Historical Note: Two TP monitors were widely used in the mainframe world and then later transitioned to the client-server world. These were CICS (customer information control system) and ACMS (automated code management system).

Application Integration Middleware Servers and Services

Application integration middleware provides interfaces to a wide variety of applications. Application integration middleware might be a service that enables running a legacy system through a thin-client browser or a service that enables the execution of multiple application functions from an integrated user interface. The methods used to achieve this integration include application program interfaces (API), remote procedure calls (RPC), and object request brokers (ORB).

Protocols and services related to application integration are noted in Technology Component Standard INT-S-08. In general, those technologies listed as strategic are based on open standards.

Table INT-S-08: Application Integration Services Technology Component Standard *Updated 10-1-2008*
Strategic:
Object Request and Request Broker Protocols/Suites .NET Remoting SOAP over HTTP J2EE/RMI, Java 2 Enterprise Edition (the distributed version) and Remote Method Invocation Enterprise Application Integration Services (EAI) Use of Integration Servers/Services SOA Remote Procedure Calls DCE RPC DCE secure RPC (integrated with DCE security protocols for authentication, protection level and authorization) Web Services Object and Application Interfaces IDL (interface definition language) stubs; MIDL (Microsoft); OMG IDL; DCE IDL
Emerging:
None
Transitional/Contained:
Remote Procedure Calls Suns' ONC+ RPC MS DCOM + (distributed common object model) OMG CORBA (common object request broker) DCE RPC DCE secure RPC (integrated with DCE security protocols for authentication, protection level and authorization) ebXML
Obsolescent/Rejected:
None
Historical Note: Fully utilizing Web Services is the recommended strategic direction when combined with an overall Service-Oriented Architecture. For a description of SOA please see Appendix A of the ETA Application Domain Report, *Example SOA Centralized Implementation and Governance Model*. Other methods, such as DCOM and CORBA are still used and recommended for specific scenarios.

Enterprise Service Bus

An enterprise service bus (ESB) is a Web-services-capable middleware infrastructure that supports communication and mediates application interactions. To be an ESB, a middleware subsystem must

1. implement program-to-program communication (always supporting Simple Object Access Protocol/Hypertext Transfer Protocol [SOAP/HTTP], and almost always supporting SOAP on message-oriented middleware [MOM] and plain MOM);
2. support other Web services standards (including Extensible Markup Language [XML] and Web Services Description Language [WSDL]);
3. be capable of service discovery, binding and virtualization (transparently substituting alternative service providers) and intelligent message routing;

4. have an extensible, intermediary-based architecture so that additional features can be plugged in; and
5. have an awareness of message schemas through the use of metadata. [4]

Instant Messaging

Instant Messaging[5] is the exchange of text messages through a software application in real- time. Generally included in the IM software is the ability to easily see whether a chosen friend, co-worker or "buddy" is online and connected through the selected service. Instant messaging differs from ordinary e-mail in the immediacy of the message exchange and also makes a continued exchange simpler than sending e-mail back and forth. Most exchanges are text-only, though popular services, such as AOL, MSN Messenger, Yahoo! Messenger and Apple's iChat now allow voice messaging, file sharing and even video chat when both users have cameras.

Products and services related to instant messaging are noted in Technology Component Standard INT-S-09. In general, those technologies listed as strategic are based on open standards.

Table INT-S-09: Instant Messaging Technology Component Standard *Added 10-1-2008*
Strategic:
IBM Lotus Sametime Jabber XCP Microsoft Live Communications (Server/Office Communication Server)
Emerging:
Bantu EIM Parlano MindAlign Sun Microsystems Java System Instant Messaging
Transitional/Contained:
Novell GroupWise Messenger
Obsolescent/Rejected:
None

Mashup

A "mashup"[6, 7] is a lightweight, tactical presentation layer integration of multi-sourced applications or content into a single, browser-compatible offering. Mashups[8] currently come in three general types: consumer mashups, data mashups, and business mashups.

[4] Integration Suites and ESBs: Integration Technology for the Mainstream. Jess Thompson & Roy Schulte. Gartner Research.
[5] Wikipedia, April 2008: http://en.wikipedia.org/wiki/Instant_Messaging
[6] The source for much of the information presented in the Mashup sections was obtained through Gartner Research, Gartner, Inc. Stamford, CT.
[7] Anthony Bradley, Daniel Sholler, David Gootzit. *Enterprise IT Departments Must Prepare for the Impact of "Mashups"* 7 September 2007 Gartner Research: ID G00151424 Retrieved November 2007.
[8] Wikipedia: http://en.wikipedia.org/wiki/Mashup_%28web_application_hybrid%29. Retrieved November 2007.

Mashups[9] leverage content and logic from other Web sites and Web applications, and are built with a minimal amount of code (which can be client-side JavaScript or server-side scripting languages, such as PHP or Python). Mashups aren't intended to be strategic, systematically built, industrial-strength enterprise applications; rather, they're created quickly or opportunistically to meet a focused tactical need. Mashups are generally personalized to fulfill personal productivity needs rather than the requirements of a long- standing corporate role.

Protocols and services related to mashups are noted in Technology Component Standard INT-S-10. In general, those technologies listed as strategic are based on open standards.

Table INT-S-10: Technology Component Standard *Added 10-1-2008*
Strategic:
Ajax **-** AJAX (Asynchronous JavaScript and XML) is a group of interrelated web development techniques used for creating interactive web applications. EDA - Event-driven architecture SOA - Service-oriented architecture WOA - Web-oriented architecture URI - Uniform resource identifiers Rest - Representational state transfer ATOM - the Atom Publishing Protocol is a simple HTTP-based protocol for creating and updating web resources. RSS - RSS (Really Simple Syndication) is a family of Web feed formats used to publish frequently updated content such as blog entries, news headlines or podcasts. Use available API's wherever possible http://www.programmableweb.com/apis/directory/1?sort=mashups
Emerging:
None
Transitional/Contained:
None
Obsolescent/Rejected:
None

[9] Wikipedia: http://whatis.techtarget.com/definition/0,,sid9_gci1167147,00.html. Retrieved December 2007

Service-Oriented Architecture Development

Service-Oriented Architecture (SOA) addresses the requirements to help ensure SOA-based services are designed to meet agency and state business needs and are architected for Tier One[10] (T-1) enterprise use.

Domain-wide Requirements

The following domain-wide requirements pertain to all components in the Service-Oriented Architecture.

Service Conditions and Planning Design Service

Conditions

SOA-R-01:	**Tier One Services** [11] **(T-1)**. All Tier One services shall be published on the state Service Offering and Support Center (SOSC) service registry, once it is created.
SOA-R-02:	**T-1: Service Componentization.** Services shall have well defined interfaces, shall not share state, and shall communicate by messages.
SOA-R-03:	**T-1: Service Autonomy.** Services shall have authoritative control over the logic they encapsulate.
SOA-R-04:	**T-1: Service Optimization.** Services shall be constructed modularly, coded unambiguously, be highly secure, and designed for high performance and scalability.
SOA-R-05:	**T-1: Service Encapsulation.** The internal mechanisms and data structures of a service shall be hidden behind a defined interface. Service encapsulation separates the contractual interface from its implementation.

Module Services

SOA-R-06:	**T-1: Loosely Coupled.** Services shall be designed to be loosely coupled.
SOA-R-07:	**T-1: Interfaces.** Service interfaces shall be clearly defined and documented.
SOA-R-08:	**T-1: Interface Metadata.** Developers shall enter interface metadata or use tools to generate interface metadata that specifies an explicit service contract so that another developer can find and use the service.

[10] Tier One Definition: Services across/among agency systems. Also See: COV ITRM Glossary: http://www.vita.virginia.gov/uploadedFiles/VITA_Main_Public/Library/PSGs/PSG_Sections/COV_ITRM_ Glossary.pdf
[11] See: Definition of Key Terms – Tier Definitions

SOA-R-09: **T-1: Fully Operable Service.** Everything needed by the service to provide its functionality shall be passed to it when it is invoked. All access to a service shall be via its exposed interface. No hidden assumptions shall be necessary to invoke the service.

SOA-R-10: **T-1: Meeting Business Needs.** Business analysts and architects shall collaborate to ensure business processes are unique, well defined, and documented, and that service candidates are capable of meeting business needs and changes.

Service Modeling

SOA-R-11: **T-1: Map Service Modeling to a Business Process.** Each service shall exist within the context of at least one business process; a service plays a specific role in accomplishing a business process that achieves demonstrable business value.

SOA-R-12: **T-1: Business Process Models.** The service provider shall maintain models for business processes, as well as those for structure and behavior to indicate the roles and functions of each service.

SOA-R-13: **T-1: Individual Service Description**. The description of each service shall include the business process model(s) for which the service was designed. This description may be maintained manually and shall be available on the state's service repository for Tier One services.

SOA-R-14: **T-1: Service Contextual Summary.** The description of each service shall include a contextual summary that establishes the name of the service and a brief (single paragraph) description of the real world effect of using the service.

Distributable Modules

SOA-R-15: **T-1: Distributed Modules.** The service components shall be able to run on disparate computers and communicate with each other by sending messages over a network at runtime.

SOA-R-16: **T-1: Service Contract.** The service provider shall be responsible for creating a Service Contract for each service and negotiating with each service consumer. Service contracts shall be posted on the state SOA Services Registry to communicate information about the service.

SOA-R-17: **T-1: Enterprise Architecture Standard (EA225-).** In addition to complying with the ETA SOA Topic Report, service providers and consumers shall follow the EA Standard (EA225-) for service application, integration, service bus, and messaging requirements.

SOA-R-15: **T-1: Distributed Modules.** The service components shall be able to run on disparate computers and communicate with each other by sending messages over a network at runtime.

SOA-R-16: **T-1: Service Contract.** The service provider shall be responsible for creating a Service Contract for each service and negotiating with each service consumer. Service contracts shall be posted on the state SOA Services Registry to communicate information about the service.

SOA-R-17: **T-1: Enterprise Architecture Standard (EA225-).** In addition to complying with the ETA SOA Topic Report, service providers and consumers shall follow the EA Standard (EA225-) for service application, integration, service bus, and messaging requirements.

Discoverable Modules

SOA-R-18: **T-1: Services shall be clearly defined and documented.** Services shall be easily identified by their purpose, and easily found by other agencies. Software developers shall write or generate interface metadata that specifies an explicit service contract, so other developers can find and use the service.

SOA-R-19: **T-1: Centralized Service Offering & Support Center (SOSC)** – A centralized support center shall be built and empowered within the Virginia Information Technologies Agency (VITA) as the approach to structured application integration matures.

SOA-R-20: **T-1: Commonwealth SOSC SOA service registry.** The state's SOSC service registry shall be an online catalog that contains the names and information about each service, including associated attributes like metadata.

SOA-R-21: **T-1: Mandatory use of SOSC SOA Services Registry.** Once designated as Tier One, services shall be registered in the state SOSC SOA Services Registry in order to enable discovery, minimize redundancy of duplicate services, and maximize reuse.

SOA-R-22: **T-1: Software interface definitions.** Software interface definitions shall be maintained in the state's SOSC SOA Services Registry so they are available to application developers.

SOA-R-23: **T-1: Mandatory review of SOA requirements.** Agency Providers with Tier Two services that are likely candidates for adoption by other agencies shall review these standards before registering services in the state SOSC Service Registry. Agencies are encouraged to publish services for reuse. In order to be designated as Tier One, these services shall meet the design and governance conditions in the SOA Topic Report which establish requirements for qualifying Tier Two candidates.

Service Naming

SOA-R-24: **T-1: Unambiguously service naming.** Services shall be uniquely identified, secured and versioned. Services shall be unambiguously named based upon their purpose and to best represent the task in what is known as the real world effect. Services usually map to a business task.

SOA-R-25: **T-1: Service real world naming.** The name of the service shall encapsulate

the essential aspects of the real world effect of the service; that is, the name of the service shall represent what the service accomplishes (in business terms), rather than how the service works.

For example "verify zip code, verify correct address" are representations of services based or named after the real world effect and are easily understood by business and technical staff.

SOA-R-26: **T-1: Prohibited naming.** The name shall not indicate the underlying information system that implements the service, nor the agency or organization that provisions the service, nor any technical details about how the implementation works.

Notes: Additional service naming conventions may be developed by the multi-agency governance teams.

Service Description

SOA-R-27: **T-1: Real world description of the service accomplishes.** Services shall contain a complete description of the real world effect of the service.

SOA-R-28: **T-1: Action list and description of the services.** Services shall contain a list and brief (single paragraph) description of each of the actions that can be performed on the service.

SOA-R-29: **T-1: Principal information and entities list and description of the services.** Services shall contain a list and brief (single paragraph) description of the principal information and entities involved in interaction with the service via its actions.

SOA-R-30: **T-1: Metadata categories and values of the services.** Services shall contain a list of the principal metadata categories and values for the service (a future version of these standards or related guidelines may specify a standard set of metadata categories for services, based on experience implementing the integration architecture.

SOA-R-31: **T-1: Description of the business effect of the services.** All aspects of the description shall be free of any implementation details or dependencies. The description shall not refer to particular databases or systems in the description of the real world effect; rather, the description shall describe the business effects of the service.

Service Metadata

SOA-R-32: **T-1: Service interface definition.** Each service interface shall have a complete definition that captures its semantic meaning.

Each attribute shall identify its data type and other parameters that specify the range of its values.

SOA-R-33: **T-1: Metadata categories.** Each service interface shall have a set of metadata categories and values, as appropriate, to define the context of the element.

SOA-R-34: **T-1: Metadata provider and service version.** The metadata for a service shall include the service provider that owns and governs the structure of the service and the current version of the service and messages.

SOA-R-35: **T-1: Service interface name.** The name of each service interface shall encapsulate the meaning of the service in a way free of any reference to implementation detail.

SOA-R-36: **T-1: Registered metadata identifier.** Each exposed class and service interface shall include an identifier in service's registered metadata.

Swappable Modules

SOA-R-37: **T-1: Swappable Module Designs.** The design of the service module shall allow it to be replaced by another module that offers the same service without disrupting modules that used the previous module. This is accomplished by separating the interface design from the module that implements the service.

SOA-R-38: **T-1: Internal services.** Services that make functionality or information available to other services shall do so through separate well defined interfaces.

SOA-R-39: **T-1: Module replacement.** Services shall be designed so that modules may be replaced without affecting the consumers.

SOA-R-40: **T-1: Minimize dependency on other systems.** Services that use functionality or information provided by other systems or services shall access that functionality or information in a way that minimizes dependencies on those other systems' implementation details.

Shareable Service Modules

SOA-R-41: **T-1: Service shall be invokable from disparate applications.** Services shall be designed and deployed in a way that enables them to be invoked successively by disparate applications in support of diverse business activities.

SOA-R-42: **T-1: SOSC service registry posting.** The service shall be posted to and made available on the state SOSC registry once designated as Tier One.

SOA-R-43: **T-1: Service provider responsibilities – development and implementation.** The service provider is responsible to ensure

the service follows the requirements of the SOA design process while under development and implementation.

SOA-R-44: **T-1: Service provider responsibilities – changes.** The service provider is responsible to ensure changes to the service follow the requirements of the SOA governance and Consumers are made aware of all changes.

Service Features Security

SOA-R-45: **T-1: Design security.** Each service shall be designed to ensure provider and consumer security.

SOA-R-46: **T-1: Service audit.** Services shall have the ability to be audited (also see Service Metrics.)

SOA-R-47: **T-1: Vulnerability testing.** Vulnerability testing shall occur before services are deployed.

SOA-R-48: **T-1: Legacy system vulnerability testing.** Services that interface with legacy systems shall also ensure the systems are not exposed to vulnerable security threats or breaches.

Scalability

SOA-R-49: **T-1: Scalable Architecture.** Service providers shall architect the service so it is scalable to meet current and future consumer needs.

SOA-R-50: **T-1: Service capability and capacity.** The provider shall identify the service capability, capacity, expected number of users, and the number of transactions per minute.

SOA-R-51: **T-1: Designed capacity.** Services shall be designed to handle the number of users per each Service Level Agreement and architected to be scalable to several times the number identified in its current configuration.

Availability

SOA-R-52: **T-1: Service availability.** The service component architecture shall be highly available, and fully redundant to allow for the addition of resources without system downtime. The service shall also enable scalability of backend applications through load balancing.

SOA-R-53: **T-1: Scheduled maintenance.** Scheduled maintenance periods shall be identified in each SLA and service contract. Service maintenance is performed when necessary (hardware and software upgrades, software patches, faulty hardware replacement, etc.)

SOA-R-54: **T-1: Coordination of scheduled maintenance.** The service provider shall coordinate with agency consumers in advance of

scheduled maintenance that will affect agencies or users in accordance with the SLA.

SOA-R-55: **T-1: Service monitoring of availability and performance.** The service provider's technical and operational support staff shall monitor availability and performance of the service.

SOA-R-56: **T-1: Service monitoring, automated alerting and logging.** Service monitoring and automated alerting and logging shall be implemented when possible to monitor each service as well as report state and utilization.

Performance

SOA-R-57: **T-1: Service performance.** Service performance shall be monitored and reviewed to plan for the addition of resources before performance is significantly impacted.

SOA-R-58: **T-1: Monitor for increased server utilization.** Agency consumers, including backend applications shall be monitored for increased server utilization.

SOA-R-59: **T-1: Change control – testing.** Service providers and consumers shall ensure adequate testing at initial deployment and every time a change is made in the system.

Business Continuity

SOA-R-60: **T-1: Fault Tolerance.** The service shall be implemented as fault tolerant, with appropriate hardware, and software.

SOA-R-61: **T-1: System backups.** The service provider shall perform full- system backups for onsite and off-site storage on a scheduled basis.

SOA-R-62: **T-1: Business continuity.** Business continuity information shall also be included within the service contract, as well as services that require an SLA between the provider and consumers.

Problem Management

SOA-R-63: **T-1: Problem Management Responsibility and Impact.** The service provider shall be responsible for problem management and shall ensure minimal impact to service consumers.

SOA-R-64: **T-1: Notification of Maintenance.** The service provider shall establish automated triggers and scheduled maintenance through use of monitoring tools.

SOA-R-65: **T-1: Notification of Adverse Affect.** The service provider shall notify agencies of all events that have or may have an adverse affect on service delivery to customers.

SOA-R-66: **T-1: Notification of Failed Processes.** The service provider shall notify agency consumers of all failed processes.

SOA-R-67: **T-1: Seamless Problem Resolution.** The service provider shall provide seamless integration of processes that ensure agency consumer problem resolution satisfaction by tracking, alerting, escalating and solving problems.

SOA-R-68: **T-1: Help Assistance.** The service provider shall provide help assistance for consumers via an online knowledge base or Customer Service Representatives shall be available to assist by telephone.

Change Management

SOA-R-69: **T-1: Change Management Control.** All changes to the service shall follow the appropriate requirements in the Enterprise Architecture Standard (225-). Changes shall be managed to promote or provide stability and minimize the impact of the changes to the agencies.

SOA-R-70: **T-1: Change Communication.** Changes shall be planned and communicated with agency consumers and the SOA governance teams.

Service Planning

SOA-R-71: **T-1: Designated Business Owner.** Tier One services shall have a designated business owner and service provider.

SOA-R-72: **T-1: Use of SOSC Domain Service Registry.** Agencies shall check the state's SOSC Doman Service Registry to share or reuse existing SOA services before building or buying new services.

SOA-R-73: **T-1: Interoperability and Portability.** SOA-based services shall support interoperability and portability and as much as reasonably possible be independent of any specific vendor's proprietary product.

SOA-R-74: **T-1: SOA Readiness and SOA Architecture for RFPs.** Where applicable, Request for Proposals (RFP) shall require proposed vendors to identify and describe proposed solution's SOA readiness and SOA architecture.

SOA-R-75: **T-1: SOA-based acquisitions.** SOA-based acquisitions shall include language for vendor to identify its architecture and potential to loosely couple with the state's shared infrastructure and services, where applicable.

SOA Governance

SOA-R-76: **SOA Steering Committee membership.** SOA Steering Committee membership shall consist of VITA and other state agency information technology stakeholders.

SOA Technical Advisory Group

SOA-R-77: **T-1: SOA TAG membership.** SOA TAG membership shall consist of state agency architects, application developers, and business representatives or analysts to represent service providers and consumers.

Service Provider

SOA-R-78: **T-1: Designated Service Provider.** Each service shall have an agency responsible for provisioning the service. This agency is called the "service provider." The provider may represent the interests of several agencies through a program office or similar organizational unit; however, there is a single entity responsible for provisioning the service.

SOA-R-79: **T-1: Service Implementation and Function.** The provider shall be responsible for the implementation and proper functioning of the service.

SOA-R-80: **T-1: Change Management Processes.** The service provider shall follow SOSC established change management processes subject to the review and approval/endorsement of the multi- agency governance teams for Tier One services.

SOA-R-81: **T-1: Service Stakeholders.** The Service Provider shall be responsible for identifying a group of stakeholders of the service.

SOA-R-82: **T-1: Consult with Registered Stakeholders.** The provider shall ensure known stakeholders are involved in the decision process when considering changes to a service's real world effect or interface.

Infrastructure

SOA-R-83: **T-1: Infrastructure Planned Change Notices:** The SOSC shall be responsible for notifying users of the infrastructure about planned changes, consulting with users, and coordinating with users' project schedules.

Configuration Management

SOA-R-84: **T-1: Version Label Convention:** The provider of a service shall be responsible for assigning version labels to each new version of a service, according to an accepted convention.

SOA-R-85: **T-1: Posting & Notification of Version Updates.** The service provider is responsible to ensure version updates are posted to the service repository to reflect the new version and all service consumers are notified of any changes.

Assurance of Real Word Effect

SOA-R-86: **T-1: Assurance of Real World Effect.** The provider of a service shall be responsible for assuring the quality of the service, in particular making sure the service properly achieves the stated real world effect. VITA can assist the provider in fulfilling this responsibility (for example, by providing a version of the infrastructure platform dedicated to testing and service metrics for Tier One services utilizing the state Backplane), but the final responsibility rests with the provider.

Standards Conformance

SOA-R-87: **T-1: Standards Conformance.** Services identified in the state's service registry/repository or deployed on the state's SOA backplane or integration infrastructure shall conform to all Enterprise Architecture requirements and all information technology resource management policies and standards.

SOA-R-88: **T-1: Standards Conformance Responsibility.** The SOA Technical Advisory Group (TAG) and state SOSC shall be responsible for ensuring that any service deployed on the state's shared, common SOA backplane, state SOSC Domain Service Registry or integration infrastructure conforms to all Enterprise Architecture requirements and all information technology resource management policies and standards.

Service Level Agreement

SOA-R-89: **T-1: Service Level Agreement Considerations.** When establishing a service-level agreement for a service, the parties (provider and consumer(s)) shall address the following issues in the agreement:

a. Availability requirements (with what probability is the service available for interaction; provisions for negotiations and notifications for outages)

b. Responsiveness requirements (how quickly does the service respond, both synchronously and asynchronously)

c. Impacts, risks to enterprise and agency services, data stores, and systems.

d. Privacy requirements (what restrictions are there on what the parties may do with information that they obtain as part of the service interaction)

e. Change management processes.

f. Funding model or cost model.

g. The provider of a private service shall negotiate change management processes with consumers of the service.

h. Under what conditions (including how often) a provider may change the service's interface.

i. How far in advance of a proposed change the provider shall notify consumers of the intent to change.

j. How to resolve disputes between consumers regarding the viability or desirability of a change to the interface.

k. How the partners will fund and implement system changes that result from the interface change.

Service Reuse

SOA-R-90: **T-1: Duplicate Service or Interface Restriction.** Services and interfaces shall be designated as Tier One common assets upon demonstration of a clear business case; once designated as such, a business case is required for an agency to invest in and provide a duplicate service or interface.

SOA-R-91: **T-1: Reuse Process.** Processes for developing and defining Tier One services for reuse shell be defined by the SOA Steering Committee, SOA TAG and state SOSC as the services architecture and service metrics are documented.

State Service Offering and Support Center

SOA-R-92: **T-1: State SOSC Model.** The state SOSC model shall maximize collaboration and communication among the state SOSC and agencies. The state's SOSC also shall support the state SOA backplane with service registry, infrastructure, and system integration.

SOA-R-93: **T-1: State SOSC Monitoring and Support.** The state SOSC shall maintain and monitor the state's SOA backplane and integration infrastructure.

SOA-R-94: **T-1: Service Metadata.** The SOSC shall assist agencies/service providers assemble and maintain service documentation (service metadata) for the application interactions.

SOA-R-95: **T-1: SOSC Registry/Repository.** The state SOSC shall maintain a single statewide registry/repository of Tier One SOA- based services and system interfaces.

SOA-R-96: **T-1: Format Consistency.** The SOSC and multi-agency SOA TAG shall work with service providers to ensure service models are consistent in format and content across the enterprise, ensure that each model contains proper, consistent metadata, ensure the owner agency is identified as accountable for the service, and ensure that models reflect the reuse of existing services to meet the needs of new projects.

SOA-R-97: **T-1: Service Metrics.** Each service shall have a set of metrics to measure its performance and reuse. Service metrics shall provide quality of service, performance, and reuse information for investment, design, deployment, and maintenance planning.

SOA-R-98: **T-1: State SOA Backplane.** The state's SOSC is responsible for provisioning the state SOA backplane. The SOA backplane shall include mechanisms for lifecycle management such as registry/repository, policies, and service orchestration; business analytics for service metrics, development tools for security, management, and adapters; and communications for routing, naming, quality of service, and transformation.

Section 5.5 - ETA Networking and Telecommunications Domain

The networking and telecommunications standards address infrastructure and services architecture requirements for executive branch agencies in the Commonwealth of Virginia. These standards provide requirements that will assist agencies in meeting their current needs while moving towards the future vision for networking and telecommunications in the Commonwealth. For networking and telecommunications, the future vision is simple. Future networks will be highly integrated and will accommodate numerous end-to-end services that will coexist in this integrated infrastructure. Conceptually, the future network for participating agencies will be one network.

The networking and telecommunications architecture addresses two topics: facilities telecommunications infrastructure and telecommunications. Facilities telecommunications infrastructure addresses the cabling, pathways and documentation that are tied to a physical location (e.g., building, office space, outdoor space, or campus of buildings). Telecommunications addresses all other infrastructure and services, whether provided by the Commonwealth or by external service providers. Included in services are Local Area Networking (LAN), Wide Area Networking (WAN), and other telecommunications services (e.g., phone, data, multimedia).

Domain-wide Requirements

The following domain-wide requirements pertain to all topics and components in the Network and Telecommunications Domain:

NET-R-01 **Notifications Required for Networking and Telecommunications Changes Due to Agency Facility Changes.** Agencies planning facilities changes must provide timely notification to appropriate networking and telecommunications authorities to ensure the availability of business critical telecommunications and networking services. Networking and telecommunications infrastructure requirement changes are an integral part of agency office change plans, whether the changes involve moving, expansion, construction, renovation, or lease changes Agencies served by VITA that are planning changes must involve VITA in the early planning to determine the lead time required. When state-owned or state-leased buildings are involved, agencies must notify the Department of General Services, Division of Engineering and Buildings. When local government-owned buildings are involved, agencies must notify the local government entity responsible for networking and telecommunications.

Rationale:

Notifications to involved government authorities helps to avoid delays and inflated expenses. Agencies need to provide a six month advanced notice for minor changes and an eighteen month notice for major changes to ensure that delays will be avoided.

NET-R-02: **Inter-building Connections.** Agencies, except for institutions of higher education, which require network interconnections between two or more buildings, shall work with VITA to determine a solution. The Department of General Services, Division of

Engineering and Buildings shall be a participant in the discussion whenever Commonwealth owned or leased buildings are involved. The local government shall be a participant in discussions whenever local government owned or leased buildings are involved.

NET-R-03: **Single Pipeline Planning Data.** Agencies are required to report *state to local* connectivity information and connection usage data when requested by the Commonwealth's Chief Information Officer (CIO). Such reporting requirements must have pre-defined, decision-based uses.

Rationale:

The future network vision for the Commonwealth includes reductions in state required connectivity costs for local governments, local government agencies, local branches of state courts, and branch offices for state agencies. The enterprise network redesign shall include considerations of a simplified design for required local connectivity, which is often referenced as a "single pipeline" between state and local government. To consider possible single pipeline solutions for the Commonwealth, requirements must be assessed.

Facilities Telecommunications Infrastructure

This topic addresses requirements for infrastructure that is typically used by an agency but not owned by the agency. When an agency is occupying a facility, it will have use of the building cabling, electrical systems, and access closets that together constitute much of the physical portion of the agency's premises networking and telecommunications solution. Facilities telecommunications infrastructure is currently limited to cabling plants and their documentation. In the future, wireless infrastructure may become a common part of the infrastructure typically provided as part of a facilities lease and remaining with the facilities at the termination of a lease.

NET-R-04 **Cabling Requirements.** Agencies must ensure the availability of standards-based structured cabling systems for all agency telecommunications in agency occupied space. Agencies must ensure the deployment of ANSI/TIA/EIA (American National Standards Institute/Telecommunications Industry Association/Electronic Industries Alliance) standards-based designs, topologies, components, distances, installation methods, cable testing, and cable administration. All related minimum requirements or mandatory criteria that must be met (unless exceptions are noted in this document) are addressed in the following Commonwealth-adopted international standards (ANSI/TIA/EIA standards):

- **ANSI/TIA/EIA 568-B.1, Commercial Building Telecommunications Cabling Standard, Part 1: General Requirements.** This standard addresses cabling infrastructure design, installation and field testing for horizontal cabling, backbone cabling, and work areas. It also covers requirements for telecommunications rooms, equipment rooms, and entrance facilities. This standard

recommends the use of ANSI/TIA/EIA T568A, which specifies the wiring scheme to be used with the RJ-45 modular plug (8 position jack) and optionally allows use of T568B. The 568-B.1 standard is typically used in conjunction with the National Electric Code to provide an appropriate cable plant.

Exceptions

Agencies except for institutions of higher education shall ensure use of the ANSI/TIA/EIA T568A wiring scheme for RJ-45 modular plugs in agency occupied space and shall not use T568B. Agencies are required to use T568A consistently throughout their cabling plant. T568A provides backwards compatibility with both one- pair and two-pair USOC (Universal Service Order Code) wiring schemes.

Institutions of higher education, which prior to 1991 cabled their entire campus using the T568B wiring scheme (pin pair assignment), may continue using T568B without an exception. Other agencies require an exception for any new installation of cabling using T568B except when the installation is accommodating the needs of existing users.

Agencies that have mixed T568A and T568B cabling plants are required to carefully document (see ANSI/TIA/EIA-606-A) the mixture and have clear rules for adding or partially replacing cabling in a building. In addition, an agency with a mixed plant must have a plan for switching to T568A as building cabling is replaced.

When an agency is replacing all horizontal cabling, the agency is required to implement the T568A standard.

- **ANSI/TIA/EIA 568-B.2, Commercial Building Telecommunications Cabling Standard, Part 2: Balanced Twisted Pair Cabling Components.** Addresses specifications for horizontal four-pair cables and backbone multi-pair cables and components. All Category 6, Category 5e and Category 3 cable specifications and testing are addressed.

Exception

Agencies must ensure a minimum of certified Category 5e cable when installing new or replacement telecommunications horizontal cabling in agency occupied space.

- **ANSI/TIA/EIA 568-B.3, Commercial Building Telecommunications Cabling Standard, Part 3: Optical Fiber Cabling Components Standard.** Addresses multi-

mode (50/125µm and 62.5/125µm) and single-mode fiber optic cabling components, transmission standards, and field testers.

Exceptions

Agencies shall use 50/125µm multi-mode fiber optic cable for all new and replacement backbone building runs. Even though 62.5/125µm multi-mode cabling is permitted in this standard, agencies shall not install this cable type in agency occupied space.

For the devices connected to the backbone fiber system via 50/125µm multi-mode fiber, agencies shall provide a minimum of four fibers (two pairs) run to each device. This will enable the use of redundant connections for equipment that may be deemed critical at a later point (e.g., implementation of Voice over Internet Protocol, VoIP). Consideration should be given to having two dark fibers (one pair) for every four active fibers (two pairs) installed, this will provide adequate backup for critical equipment if a problem occurs on one of the active pair.

- **ANSI/TIA/EIA 569-B, Commercial Building Standard for Telecommunications Pathways and Spaces.** This Standard addresses specific pathway and space design and construction practices in support of telecommunications media and equipment within buildings.

  Agencies are also required to implement all specifications in related addenda to ANSI/TIA/EIA 569-B for agency occupied office space that has an average office density (one office per 100 square feet). Pathway and room size requirements must be adjusted for higher and lower densities of telecommunications outlets or equipment than are expected in the average situation.

  Exception

  None

- **ANSI/TIA/EIA 606-A, Administration Standard for Commercial Telecommunications Infrastructure.** This standard specifies administration for a generic telecommunications cabling system that will support a multi- product, multi-vendor environment. It also provides information that may be used for design of administration products.

  Exception

When an agency alters its cabling plant, the agency must develop/maintain cable plant documentation that meets the minimum requirements of ANSI/TIA/EIA-606- A Class 3 administration as indicated in Clause 7 of the standard. In addition, agencies shall provide all cable plant documentation to the Department of General Services (DGS) central repository for cable plant documentation (see NET-R-05) using the documentation format (e.g., data names, data elements, data tables, data types, and/or spreadsheet column order) as specified by NET-R-05 and NET-R-06 below.

- **J-STD-607-A, Commercial Building Grounding (Earthing) and Bonding Requirements for Telecommunications.** The purpose of this standard is to enable the planning, design, and installation of a telecommunications grounding and bonding system which supports a multi-vendor environment and implements various system installation practices.

Exception

None

NET-R-05 **Department of General Services (DGS) Central Repository.** DGS shall provide a central repository for agency cable plant documentation (see NET-R-04, ANSI/TIA/EIA-606-A documentation). The DGS repository must be accessible to the Virginia Information Technologies Agency for planning purposes.

NET-R-06 **Cable Plant Data Formats.** The Department of General Services (DGS), Division of Engineering and Buildings, in conjunction with the Virginia Information Technologies Agency, shall provide a spreadsheet template (flat file) and optional database schema for use by agencies in providing required data to the DGS central repository. (See related requirements in NET-R-04 ANSI/TIA/EIA 606-A and NET-R-05).

Rationale:

Common data and formats are needed to ensure cable plant data can be aggregated across agencies for analysis.

Telecommunications

Telecommunications includes the hardware, software, services, and documentation related to electronic transmissions of data, voice, and multimedia content needed to conduct agency business. Components include telecommunications protocols, wired and wireless services, switches, routers and similar items. Also included are applications that provide end-to-end telecommunications services such as Voice over Internet Protocol (VoIP).

Local and wide area networks are the infrastructure, signaling and services that enable numerous practical office applications including receiving and sending email, saving

documents and email, printing documents on office or workgroup printers, Voice over Internet Protocol (VoIP) telephoning, Blackberry email, always on Internet and more.

A local area network (LAN) is generally a private network. It is under the control of the owner and used by a set of related individuals and/or workgroups, typically within a single building or over a group of neighboring buildings.

A wide area network (WAN) is a geographically dispersed telecommunications network. A wide area network may be privately owned or rented, but the term usually connotes the inclusion of public networks including the public telephone system.

Telecommunications are services or applications that run on local and wide area networks. Telecommunications connect people, servers, applications tiers, businesses and more.

Protocols Requirements

NET-R-07: **LAN Protocols**. Agencies modifying their LAN services must migrate to the minimum Virginia standard of IEEE 802.3 Fast Ethernet (100 Mbps Switched Ethernet) or to a higher bandwidth Ethernet service (e.g., up to 802.3an 10GBASE-T 10 Gbit/s (1,250 MB/s) Ethernet over unshielded twisted pair (UTP)).

NET-R-08 **IP Access to LAN Nodes.** Agencies must ensure that each agency LAN node and LAN segment may be accessed using IP addressing. This mandatory requirement was to have been met in December of 2003.

NET-R-09 **Routing.** Agencies must employ IP as the standard addressing protocol for all routed transmissions. Agencies establishing new and replacement connections to external business partners, local governments, and state agencies must employ IP addressing. If other protocols are used as a transitional strategy, when routed, these protocols must be tunneled through IP.

Switches, Routers and Similar Items Requirements

NET-R-10 **Network Hardware.** Agencies acquiring new network hardware (i.e. firewalls, routers, switches, etc.) must ensure that the devices are Simple Network Management Protocol (SNMP) compliant.

NET-R-11 **SNMP Use.** All agencies that manage networks must employ SNMP-compliant (Simple Network Management Protocol compliant) device management. SNMP is a protocol that enables management information for a network element such as a switch to be inspected by a remote manager.

NET-R-12 **Networking Devices.** Agencies and their network service providers who establish contracts for 500 or more of a single network device type (e.g., a particular router, switch or hub), must have validated performance and cost comparison data (e.g. price, quality, availability, service quality, reliability and support costs) for a second brand for the device type during a particular

acquisition cycle. This data may be obtained from a small- dedicated network segment, a separate network, or from a third party (e.g. University, local government, etc.). The intent is that the Agencies or their service providers be able to use comparison results in acquisition and maintenance negotiations.

NET-R-13 **IP Addresses in the Enterprise Network.** Agencies served by any portion of the VITA enterprise network shall acquire IPv4 address space from VITA or gain VITA approval for using its own address space. Any served agency with its own address space must notify VITA of the address space renewal date. No served agency may increase their use of RFC1918 addresses without also using route distinguishers (i.e., VPN-IPv4 RD). Any served agency currently using the private address range (RFC1918) must record this use with VITA and prepare to discontinue this use when the served agency's network is integrated with other agencies' networks for the purpose of common management. Served agencies are required to use only registered IPv6 addresses assigned by VITA when they switch to IPv6. Also, VITA reserves the right to revoke and reassign address space as dictated by future network designs.

Notes: An RFC is a document distributed as a request for comments. In many instances, RFCs are treated as industry standard recommendations. Many standards groups issue RFCs.

VITA must provide agencies with assurance that recorded IP address information will not be shared with anyone who may be required to divulge the information to the public.

Wired and Wireless Services Requirement

NET-R-14 **VoIP.** Agencies implementing VoIP must provide well-ventilated and air-conditioned premises wiring closets to protect investments and to ensure services.

Virginia Government Internet Domain Naming

Government Internet domain naming identifies and implements standardized naming conventions to aid in developing statewide electronic directories and reducing overhead and administrative costs.

Domains and sub-domains of other domains are often referred to by level. The levels of a domain name are numbered from right to left. Using the sample domain name department.oaa[12].virginia.gov the levels are as follows:

- first-level gov
- second-level virginia
- third-level oaa
- fourth-level agency's discretion (web-site application name, activity name, department names, etc.)

[12] oaa = official agency acronym (e.g., VITA)

NET-R-15 **Virginia.Gov Mandated Use –** All executive branch agencies in the Commonwealth except for institutions of higher education shall use the "virginia.gov" domain name. This requirement does not preclude agencies from possessing other domain names for which they separately register and accept full responsibility.

NET-R-16 **Domain Name Structure –** Domain Names are to be composed of alphabetic characters and numbers. Upper/lower case is transparent. Hyphens (dashes) are allowed but may not be used at the beginning or end of a domain name. Within a domain name spaces, the underscore, and special characters are not permitted. Special characters include, but are not limited to: ! @ # $ % ^ & * ( ) ? "

NET-R-17 **Third Level Domain Names – Executive Branch Agencies –** The name of an agency of the Commonwealth of Virginia will be at the third level and will consist of the official agency acronym/abbreviation.

Example:

a. vita.virginia.gov
b. doa.virginia.gov

NET-R-18 **Fourth Level Domain Names –** The fourth level of the "virginia.gov" domain will be used to further subdivide the entities established at the third level. Because many organizations exist at several levels of government, their location within this hierarchy will allow citizens to distinguish between them. Fourth level names are generally at the discretion of the requesting agency. The examples below are offered as a guideline to encourage a generally accepted and recognizable naming convention.

Examples of Departments or Activities of Executive Branch Agencies:

a. license.dgif.virginia.gov
b. eVA.dgs.virginia.gov

Technology Tables for Networking and Telecommunications

The technology component standard tables below provide strategic technology and service directions for agencies that are acquiring technical components or services for local area networking, wide area networking or other telecommunications. Agencies *might be acquiring* these components via purchasing, space rental leasing, facilities construction or modification, or other acquisition methods. Both wired and wireless components and services are addressed. Subtopics are noted in table headings.

Table NET-S-01: Wired Local Area Networks (LANs) Technology Component Standard *Reviewed October 1, 2008*
Strategic:
IEEE 802.3 Fast Ethernet (100 Mbps Switched Ethernet) Higher bandwidth Ethernet service (802.3 Full duplex Fast Ethernet, 802.3ab Gigabit Ethernet over copper, 802.3ad, or 802.3z Gigabit Ethernet over fiber) *10 Gigabit Ethernet LAN (little need but becoming highly cost effective—see FTTE-H) VoIP Centrex (cost reductions)* Note: Category 5e LAN is the minimum required for enabling VoIP.
Emerging:
Transitional/Contained:
Ethernet 10Mbps (IEEE 802.3) ATM 25 Mbps (LANE, an element of MPOA) Note: Category 5 LAN cable is transitional because VoIP is not supported.
Obsolescent/Rejected:
Token Ring (IEEE 802.4) AppleTalk All Other Non-Strategic Protocols

Table NET-S-02: Wireless Local Area Networks (WLANs) Technology Component Standard *Reviewed October 1, 2008*
Strategic:
Wi-Fi using Access Points Frequency Hopping Spread Spectrum (FHSS, IEEE 802.11) Direct Sequence Spread Spectrum (DSSS, IEEE 802.11 and 802.11b) Orthogonal Frequency Division Multiplexing (OFDM, IEEE, 802.11a used for Access Points)
Emerging:
WiMAX (802.16e) (security and other issues)
Transitional/Contained:
Infrared (Point to Point, IEEE 802.11)
Obsolescent/Rejected:

Table NET-S-03: Cabled Wide Area Networking (WAN) Technology Component Standard *Reviewed October 1, 2008*
Strategic:
Data and VoIP example WANs Frame Relay T1 (128 Kbps-1.5 Mbps) ATM T1 (1.5 Mbps) with IMA (Inverse Multiplexing over ATM) Aggregated Frame Relay, i.e., 2, 3, or 4 T1s (3-6 Mbps) ATM DS3 (22-45 Mbps) ATM SONET (synchronous optical network) over OC3 (optical carrier) to OC12 (155- 622+ Mbps) PoS (Packet over SONET) FRASI (FR to ATM Services Internetworking) xGb Ethernet (e.g., MAN, carrier backbone) LAN speed Ethernet interconnection over public backbone xDSL (128 Kbps—8 Mbps) Cable Modem (300 Kbps—10 Mbps) MPLS VoIP Centrex
Emerging:
Transitional/Contained:
Data WAN Frame Relay 56 Kbps ISDN—narrow band (64—128 Kbps) Frame Relay DS3
Obsolescent/Rejected:

Table NET-S-04: Mobile and Remote Access to Local Area Networks (LANs) Technology Component Standard *Reviewed October 1, 2008*
Strategic:
Dial up (e.g., RAS) VPN (e.g., IP VPN) Blackberry Services *Microsoft Exchange Direct Push Mail via SPS* *Other Blackberry Competitors (Good, Nokia, Sybase)* Wi-Fi
Emerging:
Intel integrated wireless chipsets (Wi-Fi, WiMAX and HSDPA in one chipset)
Transitional/Contained:
Obsolescent/Rejected:

Table NET-S-05: Wireless Telecommunications (Voice, Image, Data, Conference, and Other Multimedia) Technology Component Standard *Reviewed October 1, 2008*
Strategic:
VITA Negotiated Services (current and anticipated services provided below) VoIP Service (using MPLS) Digital Voice, Image, Data, Centrex and PBX Digital Cellular Service: 800 MHz, CDMA, WCDMA, CDMA 2000, CDMA EV-DO, GSM/GPRS PCS Service: (1900 MHz, personal communications services—Sprint, digital wireless) *Cingular or* Ntelos Service: GSM/GPRS) this is not cellular but provides cell-type services at a different frequency; uses trimode phones (1900/800 MHz, analog and digital) Nextel Service: 800 MHz iDEN; wireless telephone service (note: this is not cellular but is Enhanced Specialized Mobile Radio (ESMR)—2 way radio) Analog Voice, Centrex, PBX (still strategic for some locations) Wi-Fi (802.11a,b,g)
Emerging:
VoIP Wireless (high mobility in building is a place to start—e.g., forensic lab, corrections, hospital)
Video Conference over IP VoWLAN (802.11r) WiMAX (802.16e) WLAN (802.11n) High speed uplink and downlink, HSDPA QoS for voice/video 802.11e, WSM an WME Mesh Networks Wireless Video Conferencing Wireless PBX 200 Mbps WLAN links IP Multimedia, IMS and SIP Fixed mobile convergence service
Transitional/Contained:
Analog Cellular (AMPS)
Mobitex is currently a Cingular packet data service that uses MASC protocol and has a limited service area (9.6—19.6 Kbps)
Obsolescent/Rejected:
CDPD

Social Media Use

Social media is a new topic in the Enterprise Technical Architecture (ETA) Networking & Telecommunication Domain Report. The requirements in this section of the EA Standard describe technical topics such as wikis, blogs, mash ups, web feeds (such as Really Simple Syndication [RSS] feeds[13]), moderated discussion tools, social networking sites and virtual worlds.

The social media requirements create an overall framework for executive branch agencies to use when:

- determining whether to engage in social media efforts; or
- considering whether their social media use follows requirements.

The team that developed the Social Media Topic Report consisted of representatives from VITA and several Commonwealth of Virginia executive branch agencies. Its members, who met over a 10-month period, are experienced in social media, IT, web development and programming, marketing and communications. They use social media tools every day, personally and professionally.

The complete Social Media Topic Report is available on the EA Library page in the VITA website at: http://www.vita.virginia.gov/oversight/default.aspx?id=365. The report discusses principles, recommended practices, requirements and their rationale.

Topic-wide Requirements
The Social Media Topic Report team identified the following topic-wide requirements.

SOC-R-01 **Enterprise Application Compliance –** Agencies shall ensure that their use of social media complies with applicable standards, such as the Enterprise Architecture Standard (EA*225-series*), Virginia Information Technology Agency Accessibility Standard (GOV103-*225-series*), the Information Security Policy (SEC519-*225-series*), all Information Security Standards (SEC502-series) and other security related requirements.

SOC-R-02 **Prohibited Topics –** Agencies shall avoid:

a.) Engaging in *publishing and or sharing* vulgar or abusive *content*, personal attacks of any kind, or offensive terms targeting individuals or groups.
b.) Endorsement of commercial products, services or entities. c.) Endorsement of political parties, candidates or groups.
d.) Lobbying members of the General Assembly using agency resources.

SOC-R-03 **Be a Good Custodian** – Social media use requires the agency to be a "good custodian," one that posts regularly, moderates comments as appropriate and checks often for *content* ~~messages~~ that may require a response.

[13] Often called Rich Site Summary

SOC-R-04 **Records Retention and Disposition** - Ensure that *content* ~~information~~ is created, kept and, if necessary, disposed of in accordance with agency policies and the Library of Virginia public records retention and disposition schedules.[14]

SOC-R-05	**Freedom of Information Act (FOIA)** - Content posted to social media channels, is subject to the Commonwealth's Freedom of Information Act (§ 2.2-3700 et. Seq. of the *Code of Virginia*) at: law.lis.virginia.gov/vacode/title2.2/chapter37/. All public records are presumed to be open and may be withheld only if a statutory exemption applies. FOIA requests may cover social media content and/or be submitted via social media channels.
SOC-R-06	**Use of Electronic Communications and Social Media (DHRM Policy 1.75) –** Agencies shall ensure their use of social media complies with the DHRM Policy 1.75 "Use of Electronic Communications and Social Media."[15]
SOC-R-07	**Document Business Case -** Agencies using social media shall have a written business case for each social media platform that clearly defines goals, measurement standards, target audiences, benefits, approval processes, risks and resources. The agency must also include in the business case an internal employee social media policy and external commenting policy.
SOC-R-08	**Follow All Applicable Laws** – An agency shall adhere to all applicable laws, including state records law, copyright and other intellectual property law, and constitutional and statutory limitations regarding speech.
SOC-R-09	**Safeguard Sensitive Information** – Agencies shall not share or post sensitive information, such as personally identifiable information. Do not publish or report on conversations that are meant to be pre-decisional or internal, unless given permission by management. *Agencies shall alert users to not submit personal information.*

Business and Service Needs

Before implementing social media initiatives, it is important to consider whether social media will assist in meeting an agency's business and service needs and goals. Agencies shall determine whether there are existing social media channels being employed in the agency. If so, determine how each platform, channel and/or group fits into the overall communications strategy of the agency.

The Social Media Topic Report team identified the following business and service needs technical topic-specific requirements:

[14] Virginia Public Records Act. law.lis.virginia.gov/vacode/title42.1/chapter7/ Retrieved 2014-12-04 [15] Use of Electronic Communications and Social Media (DHRM Policy 1.75), www.dhrm.virginia.gov/hrpolicy/pol175UseOfInternet.pdf. Retrieved 2013-12-12

SOC-R-10	**Identify Existing Channels** – Agencies shall determine whether there are existing social media channels being employed in the agency *or by external entities and or partners*. Determine how each platform, channel and/or group fits into the overall communications strategy of the agency.
SOC-R-11	**Define Goals -** Before expending time, effort and resources, the agency shall decide why and how social media will be used to meet business and service goals.

SOC-R-12 **Define Audiences –** Agencies shall define any and all current and potential audiences. This determination can affect the social media *platform* chosen.

Rationale:
Social media can have a variety of audiences, such as:

- stakeholders;
- vendors;
- employees;
- legislators;
- media;
- executive branch agencies; and/or
- residents and visitors.

Business Case

The business case should include the rationale and justification for selecting social media as a communications channel, together with relevant risks and mitigations. As with all other channel evaluation, it is important to consider the context in which it will be applied and how that will contribute toward achieving the agency's overall strategic aims.

The suggestions here aim to stimulate thinking around some of the key areas for consideration when planning to use social media and may be used to form the business case document for the agency.

The Social Media Topic Report team identified the following business case topic-specific requirements:

SOC-R-13 **Create a Social Media Plan –** Agencies shall create a written social media plan:

a.) include a risk assessment to address opportunities, challenges and weaknesses per the Commonwealth's IT Risk Management Guidelines (SEC506-series);[16]
b.) identify goals;
c.) identify target audience(s);
d.) predict and plan for potential audience reactions and interactions; e.) identify, define and document roles and responsibilities;
f.) determine agency specific policies;
g.) develop clearly defined commenting policies;
h.) review resources and determine commitment/participation; and i.) determine benefits (e.g. return on investment, awareness).

SOC-R-14 **Agency Social Media Implementation and Utilization Plan –** Each agency using, or planning to use, social media shall develop a written plan.

The plan shall be reviewed and updated if needed when there is a subsequent, material change to the plan or every year (whichever occurs first).

The plan shall:

a) contain an analysis of the social media content and its compliance with related requirements identified in Social Media Topic Report;

identify by requirement number all current non-compliant items;

b) develop agency corrective action plans and schedules for correcting all non-compliant pages;

c) describe the agency's process and procedures for ensuring future content is compliant; and

d) describe the agency's continuity of operations plan, including planning for the absence of a staff member who normally manages a social media account.

SOC-R-15 **Leadership Approval –** Agency leadership shall approve the completed Agency Social Media Implementation and Utilization Plan, which includes the business case and the business plan.

Social Media Plan Example

To assist agencies with the development of their social media plan, an example is attached in the Appendences.

Implementation

[16] IT Risk Management Guidelines (SEC506-), Virginia Information Technologies Agency, www.vita.virginia.gov/uploadedfiles/VITA_Main_Public/Library/RiskManagementGuideline.pdf. Retrieved 2014-
01-06

As with the business case, the suggestions here aim to stimulate thinking around some of the key areas for consideration when planning to use social media and may be used to form the business plan document for the agency.

An Agency Social Media Implementation and Utilization Plan documents the results of the agency's analysis of its use, or planned use, of social media channels and compliance with the requirements identified in this document. It also addresses how the agency plans to bring the current or planned use of social media into compliance with those requirements and how to ensure that future use also is compliant.

The Social Media Topic Report team identified the following implementation topic-specific requirements:

SOC-R-14 **Agency Social Media Implementation and Utilization Plan –** Each agency using, or planning to use, social media shall develop a written plan, within six months of the effective date of the Social Media Topic Report.

Agencies with existing implementation plans must have them approved by agency leadership within six months of the effective date of this Social Media Topic Report. The plan shall be reviewed and updated if needed when there is a subsequent, material change to the plan or every year (whichever occurs first).

The plan shall:

a) contain an analysis of the social media content and its compliance with related requirements identified in Social Media Topic Report; identify by requirement number all current non-compliant items;
b) develop agency corrective action plans and schedules for correcting all non-compliant pages;
c) describe the agency's process and procedures for ensuring future content is compliant; and
d) describe the agency's continuity of operations plan, including planning for the absence of a staff member who normally manages a social media account.

SOC-R-15 **Leadership Approval –** Agency leadership shall approve the completed Agency Social Media Implementation and Utilization Plan, which includes the business case and the business plan.

Section 5.6 - ETA Platform Domain

The platform domain addresses requirements and technology standards for four technical topics: personal computing devices, servers, shared utility systems and desktop productivity tools.

These requirements and technology standards apply to those organizations within executive branch agencies that are responsible for supplying, managing, procuring and maintaining IT hardware, infrastructure related software, and operating systems. These organizations are hereafter referred to in the document as "Agencies with responsibilities for providing IT infrastructure".

Domain-wide Requirements

The following domain-wide requirements pertain to all topics and components in the Platform Domain:

PLA-R-40 **Security as a Platform Decision Factor –** Agencies with responsibilities for providing IT infrastructure shall ensure that proposed hardware and software platform solutions comply with the current COV ITRM IT Information Security Standard (SEC501).

PLA-R-02 **Remote Administration of Platforms –** Agencies with responsibilities for providing IT infrastructure shall acquire platforms designed for ease of remote administration, diagnosis, and systems management.

Personal Computing Devices

Personal computing devices include:

- Desktop and Notebook Personal Computers
- Personal Computer Operating Systems
- Displays
- PC Processors, Chipsets and Supported Interfaces
- Read/Write Devices
- Desktop-attached Printers, Copiers, Fax machines and Scanners
- Wireless Connectivity Devices
- Security Devices
- BlackBerrys, Smartphones and Push Email Services
- Surge Protection

The following are requirements for Personal Computing Devices.

PLA-R-03 **Centralized Personal Computing Decisions –** Agencies with responsibilities for providing IT infrastructure shall implement documented policies and procedures that control the acquisition, life cycle, security methods and techniques, connectivity and access methods, and ongoing maintenance support processes for personal computing devices.

PLA-R-38 **Personal Computing Base Images –** Agencies with responsibilities for providing IT infrastructure shall establish personal computer base images that comply with strategic office productivity and security related software technologies as defined in the COV ITRM EA Standard. These base images must also meet the minimum security requirements as defined in COV ITRM Security Standards. Customer agencies can add to these images to meet agency-specific security needs. Any changes to the base image must be recorded in a configuration management database.

PLA-R-39 **Personal Computer Base Image Extensions –** Agencies with responsibilities for providing IT infrastructure shall provide extensions to the base image to support business unit or departmental needs.

Rationale:

Increases uniformity while decreasing time and effort required to replace or deploy new systems.

Desktop and Notebook Personal Computers

The present recommended replacement life cycle timeframe for desktop computers is four to five years and for notebook computers three and one half to five years.

The following is a requirement for the Desktop and Notebook Personal Computers component.

PLA-R-13 **Replacement Life cycles for Personal Computers –** Agencies with responsibilities for providing IT infrastructure shall adopt replacement life cycles of four to five years for desktop computers and three and one-half to five years for notebook computers.

The following is a technology component standard for Desktop and Notebook Personal Computers.

Table PLA-S-06: Miscellaneous PC Components **Technology Component Standard** *Updated January 15, 2010*
Strategic:
Cardbus type PC Cards with parallel interface, DMA, and 32 bit path ExpressCard[17] —PCMCIA Cardbus replacement that provides high speed serial access embracing USB 2.0 and PCI-Express *2.0*
Emerging:
Transitional/Contained:
PC Card with parallel interface and 16 bit path*; PCI; PCI-X; AGP*[18]
Obsolescent/Rejected:

Personal Computer Operating Systems

In general, the platform architecture recommends skipping releases of software when business reasons for making a change are inadequate. The agency-side costs for making a change include the costs of testing, staff learning time, staff training, business application changes, and in some cases, the costs of lost employee productivity due to software setup and learning curves slowing daily work.

The following is a technology component standard for Personal Computer Operating Systems. This standard contains a recommended move from Windows XP directly to Windows 7. As a result of that recommendation, Windows XP Pro remains strategic, Windows Vista moves to Contained due to not being chosen for implementation, and Windows 7 is placed in emerging due to its not yet being adequately tested. It is expected that Windows 7 will move to strategic following the accumulation of adequate data from real business implementations. This is expected sooner than the usual two years following release. This decision was based on the unpopularity of Vista and the good reports on the beta and release code versions of Windows 7.

The recommendation to move Windows 7 to strategic as soon as adequate testing is completed means that agencies that provide infrastructure services and their customers will need to begin testing Windows 7 immediately. All agency and business-side applications will have to be tested, new interfaces written, hardware tested or replaced, peripherals tested or replaced, etc.

Because Microsoft will stop supporting XP in 2014, XP computers put into service after June 2009 will not have a full 5 years of support from Microsoft. This means that any PC that is used beyond the support end date will be need to be re-imaged.

[17] This technology is now implemented throughout the market place.
[18] http://www.semiapps.com/System_Functions/Digital_Interface/PCI_PCI_Express/

Table PLA-S-01: PC Operating Systems Technology Component Standard *Updated April 04, 2011 due to Microsoft release of first service pack for Windows 7*
Strategic:
Windows 7 (with tested service pack) Windows XP Pro (with tested Service Packs) until 04/08/2014 Macintosh OS X v10.x
Emerging:
Transitional/Contained:
Windows XP Pro (with tested Service Packs) after 04/08/2014 Windows Vista (the strategy is to skip this OS to save cost)[19] Macintosh OS 9.x
Obsolescent/Rejected:
Windows 2000 Professional (extended support ended 7/13/2010) Windows earlier than Windows 2000 Any home version of Windows

Displays

In the marketplace, 19 inch screens are becoming more common and have a low price. Gartner and others have suggested that the life cycle of a flat panel LCD can be 13.4 years on average[20] if the backlight does not fail). However, if there is an update or change to the operating system within the life cycle then the monitors in use must be checked for compatibility.

PLA-R-06 **Personal Computing Desktop Displays –** Display replacement decisions for all agencies including administrative units of higher education must be based on customer business needs, support considerations, cost-of-ownership data, and hardware compatibility considerations. Agencies shall ensure separate computer/display acquisition pricing.

Rationale:

Because desktop displays have a longer life cycle than the computers they support, their replacement shall not be automatic at the time of a desktop replacement.

[19] Gartner: Windows 7 Release Will Affect Vista Deployment Plans; 13 May 2009; Michael A. Silver and Stephen Kleynhans. Datamation: Nearly-50-of-IT-Shops-to-Skip-Windows-Vista; December 12, 2008; Stuart J. Johnston; http://itmanagement.earthweb.com/entdev/article.php/3790751/Nearly-50-of-IT-Shops-to-Skip-Windows- Vista.htm. Computer World: Windows 7: Why I'm Rolling It Out Early; By Shane O'Neill; May 18, 2009 04:44 PM; http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=Windows&articleId=9133206&taxonomyId=125&pageNumber=1

[20] http://www.epa.gov/oppt/dfe/pubs/comp-dic/lca/Ch2.pdf or for the whole document and appendices, see http://www.epa.gov/oppt/dfe/pubs/comp-dic/lca/ The EPA compares 15" LCD and 17" CRT monitor on life cycle related issues in Chapter 2. Backlights may fail between 4.0 and 13.4 years depending on the manufacturer, but they are field replaceable. These data are fairly old but more recent data are not available. In the report, discussions with Dell officials indicate that most of their LCD backlights have the 50,000 hour life or a life that exceeds the 13.4 years.

The following is a technology component standard for Displays.

Table PLA-S-02: Displays and Interface Components Technology Component Standard *Updated January 15, 2010*
Strategic:
Display Sizes Note: Size requirements below specify only the minimum display size that is permitted for standard desktop use. High-end needs such as GIS *and special needs* are not addressed. *An agency may have larger display sizes.*  Minimum of a 17" diagonal specification for a flat panel display when a flat panel is used for standard desktops. An example shape and size is presented on the left above. A typical diagonal measure is exactly 17". Minimum of a 20" diagonal specification for a widescreen flat panel display with a 16:10 aspect ratio. (Approximate measurements are 11" high by 16.5" wide.) An example shape is provided in the middle above. Minimum of a 19"diagonal specification for a widescreen flat panel display with a 3:2 or 15:10 aspect ratio. (Approximate measurements are 10" high by 16" wide.) An example shape is provided on the right above. *Display life cycle* *A desktop flat panel solution is to be used for its full life which may include backlight replacement.* Flat Panels A flat panel is the standard recommended replacement for desktop displays. Mouse An optical USB mouse is the standard recommended replacement to be included with a desktop. *Keyboard* *A USB keyboard is the standard recommended replacement to be included with a desktop.*
Emerging:
OLED or Active Matrix OLED (AMOLED) displays (e.g., AMOLED in iRiver Clix Gen2) *Light emitting diode displays are in higher use for small MP3/4 sized screens to large outdoor displays but still have not made a large impact in the personal computing space.*
Transitional/Contained:
Less than 17" flat panel for desktops *CRT (e.g., smaller displays may be appropriate for point of sale)* Mechanical Mouse
Obsolescent/Rejected:
CRT for desktop replacements

PC Processors, Chipsets and Supported Interfaces

Typically, the components of a computer are determined by the manufacturer with little choice on the part of the purchaser unless units are custom built. For personal computers, the Intel processors and chipsets dominate the market, but AMD and others offer equivalent business utility, often at a lower price. At present, with Office 2003 and Windows XP, most available processors and chipsets include features that exceed the needs of the typical office worker given the software they use and the way they work. A dual core processor may be helpful to users who have numerous applications running at the same time.

PLA-R-07 **Personal Computing Processors and Chipsets –** Agencies with responsibilities for providing IT infrastructure involved in acquisitions and contracts shall establish minimum bid specifications for low-end personal computers to be used by the majority of the workforce. These specifications shall include the lowest of the currently available Intel, AMD, or comparable chipsets and components that will cost-effectively meet the anticipated processing needs for productivity software, typical business needs, special needs of the mobile worker, and/or needs related to life cycle requirements. Example: the future availability of various memory options (DDR SDRAM, DDR2, DDR3, etc.) if users' memory needs increase during the life cycle of their desktops or notebooks.

Read/Write Devices

The devices addressed here are desktop and notebook devices that read from and write to transportable external media. "Writable" media for desktops and notebooks include floppies, CDs, DVDs, USB drives (which go by many names) and more.

PLA-R-08 **Personal Computing Optical Drives –** Agencies with responsibilities for providing IT infrastructure involved in procurements and contracts shall include a CD/DVD reader with CD or DVD write capabilities when establishing minimum bid specifications for desktop and notebook personal computers.

The following is a technology component standard for Read/Write Devices.

Table PLA-S-03: Read/Write Devices (Storage) Technology Component Standard *Updated January 15, 2010*
Strategic:
USB Flash Drives *USB drives typically store from 1 to 64 GB and may include security software options. With security software, they are the preferred choice for transporting sensitive files and information. These drives are recommended over CDs and DVDs for employee storage use.* A CD/DVD Combo Drives *CDs and DVDs remain popular for loading software and viewing multimedia, but are waning in popularity for storage, They have moved to external devices in the smallest form factor computers because they are not generally used but still may be required for loading software in certain cases.* External USB Hard Drives and DVD/CD drives *External drives are another option for mobile worker backups when connectivity is not available* *Blu-Ray Drives (BD-R)* *PC manufacturers now have blu-ray players in notebooks and desktops at prices around $150. However, they are not likely to be provided in the near future on a standard computer for the Commonwealth.*
Emerging:
Blu-ray BD-RW (write technologies continue to be too costly for general use. When prices decrease, this technology may become common in personal computing) (For enterprise storage use of Blu-Ray disks and DVDs, see the shared utility services technical topic)
Transitional/Contained:
Shared external *floppy drives* may be of transitional use to agencies.
Obsolescent/Rejected:
Zip Drive (Iomega) Jaz Drive (Iomega successor to Zip Drive) 5 ¼ Floppy *3.5 Floppy Drive in a PC*

Desktop-attached Printers, Copiers, Fax machines and Scanners

Some agencies tend to use large numbers of desktop-attached printers. In some cases, this usage pattern is because of continuous printing of confidential information or printing forms that require an ink signature from the customer who is in the worker's office. Others are used because a worker's job requires label printing or special document printing (e.g., certificates). As many as half of the printers presently in use across agencies are desktop attached.

The following is a technology component standard for Desktop-attached Printers, Copiers, Fax machines and Scanners.

Table PLA-S-04: Desktop Attached Printing Technology Component Standard *Reviewed January 15, 2010*
Strategic:
Laser printing devices are required for non-mobile black and white printing uses in situations where a desktop attached black and white printer must be used (Note: Desktop attached printers are strongly discouraged for most workers. See discussion in Utilities section.)
Emerging:
Transitional/Contained:
Desktop attached (non-mobile) ink-jet printers for black and white printing are to be phased out (Note: Desktop attached printers are strongly discouraged for most workers. See discussion in Utilities section.)
Obsolescent/Rejected:

Wireless Connectivity Devices

Although use of wireless technologies for mouse and keyboard connections is becoming more popular, the more typical wireless connections in Commonwealth offices are for notebook connections to the local area network in conference rooms, PDA/smartphone connections to desktops, and Blackberry connections to servers. Wireless printing is rare.

The following is a technology component standard for Wireless Connectivity Devices.

Table PLA-S-05: Miscellaneous Mobile Components Technology Component Standard *Updated January 15, 2010*
Strategic:
Receivers/transmitters for Local and Personal area networks (LAN & PAN) and mobile devices IrDA— infrared used on handhelds Bluetooth devices *2.1+EDR; 3.0* WiFi 802.11 (a+b+g)
Emerging:
WiMax Capable Devices *True Mobile 4G services from Sprint are supported by a few devices including Centrino 2, an IBM Thinkpad, and some Aircards. Devices supporting new mobile wireless WiMax standards and those in development will make this a reality in more locations if the economy permits progress. This means very high speed connectivity and data transfers in moving vehicles. Mobile 4G services are in place in the US in Baltimore (Sprint XOHM) with the next nearest (to Virginia) service to be in DC. There are no plans for services in VA at present, thus leaving this technology in the Emerging category for some time.*[21] *XOHM users have had some connectivity problems. IEEE ratification was expected in March 2009, but another RFC was created.* *802.11n WiFi Capable Devices* *Provides next generation wireless with reduced distance degradation and better multimedia streaming at higher speeds; ratification of the standard expected in the Fall of 2009 (100 Mbs). Use of devices on the market requires infrastructure replacements that are not permitted until ratified. However, devices may have n capabilities built in (e.g., notebook chipsets) as long as it is not used.*
Transitional/Contained:
PC Cards (PCMCIA) and internal devices (e.g., embedded in chipsets) that are not receiving all ratified standards including 802.11 a, b and g (to maximize wireless network design possibilities) *and soon, 802.11n* Bluetooth devices, less than *version 2.1*
Obsolescent/Rejected:

Surge Protection

All computers that are used to store valuable information should have some form of power surge protection when they are plugged in to electrical, cable, network or phone wiring.

PLA-R-15 **Surge Protection for Field Workers –** Agencies shall provide a surge protector that can protect from surges through electrical inputs including network, telephone and power lines to field

[21] Sprint's 4G Xohm WiMax: How fast is it?; By Brian Nadel; October 10, 2008 12:00 PM ET: Computer World.
http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=Mobile+and+Wire less&articleId=9116844&taxonomyId=15&pageNumber=2

workers who need to protect the data stored on their personal computers.

Rationale:

The term, "field worker" includes teleworkers, roadway inspectors, park rangers and similar workers who work outside of a networked office. Workers in networked environments typically have the needed data protection, data backups, and server UPS protections provided through their computing environments. Teleworkers typically store data continuously through Virtual Private Networks (VPNs) that connect to protected telecommunications and servers.

Servers

The platform domain addresses servers as single hardware devices and as configurations for utility service provision. Servers as hardware include the full range of computing devices from mainframe computers to small single-socket computers. The following server components are addressed:

- High-end servers including OS
- Midrange/low-end servers including OS
- Consolidation platforms

The following are requirements for Servers.

PLA-R-17 **Maintenance Agreements –** Agencies with responsibilities for providing IT infrastructure and/or service providers shall ensure that servers which support production are under a maintenance agreement for the planned life of the server. For x86 architecture, the planned life shall be a minimum of five years.

PLA-R-18 **File Servers –** Agencies with responsibilities for providing IT infrastructure shall migrate to either NAS (Network Attached Storage) or SAN (Storage Area Network) or combination whenever feasible and cost beneficial.

PLA-R-19 **OEM (Original Equipment Manufacturer) Operating Systems –** Agencies with responsibilities for providing IT infrastructure shall not use OEM provided operating systems (OS) for x86 server hardware.

PLA-R-36 **Server Capacity –** Agencies with responsibilities for providing IT infrastructure shall consider growth requirements over the server life to enable minimizing costs and reducing wasted capacity.

Rationale:

Planning may enable acquisition of a small number of large capacity memory modules instead of a large number of smaller modules and may enable avoiding excess and underused server capacity.

PLA-R-37 **Supported Server Operating Systems –** The release version levels of all server operating systems shall have vendor or equivalent level support. This support shall include security update and hotfix support. The use of unsupported open source server operating systems shall be avoided.

High-End Servers

High-end servers are defined as servers that may scale to more than 16 sockets in size and that use highly specialized architectures and processors. These mainframe-type servers typically cost more than $250,000 and have significantly greater capabilities in areas including reliability, availability, serviceability, security, privacy, business continuity provision, management consistency, and risk reduction. The operating systems such as zOS provide these characteristics. They are more scalable than midrange servers, which have similar characteristics (e.g., SMP/NUMA).

The following is a technology component standard for High-End Servers.

Table PLA-S-08: High-End Servers **Technology Component Standard** *Updated January 15, 2010*
Strategic:
Software z/OS Solaris* HP-UX AIX Windows *(may not be keeping up with hardware advances)* Linux in virtual partitions Virtual Server OSs (e.g., zVM, VMware, strategic only for: supporting OSs that are in the desired future architecture (e.g., Linux, Windows, HP-UX and Solaris* *and for* use in building test environments *Hypervisors are critical management tools for provider and agency-side cost reduction* Hardware IBM, Sun*, and HP platforms are strategic. Hardware alternatives to these platforms may be considered if they are fully compatible for running applications designed for strategic systems, provide equal or better performance for all application and architectural requirements, and introduce no problems to the Virginia architecture other than those that may be cost-effectively resolved. (Fujitsu, for example, is an alternative to Sun* for the Solaris OS) * *Note: Sun's Q3 2009 acquisition of Oracle may cause Sun's and Solaris' inclusion in "Strategic" to be reevaluated*
Emerging:
Software *Windows Virtual Server 2008 R2 Hyper V*
Transitional/Contained:
Software Unisys OS2200 VMS Unix other than Solaris, AIX, Linux, and HP-UX Virtual Server OSs used to support older versions of a strategic OS in cost-effective consolidation transitional plans *OS 5i (formerly OS/400)* Hardware IBM ES9000 (9221)
Obsolescent/Rejected:
Software MVS XA MPE *OS/400 (library OS) MVS* *OS/390*

Midrange to low-end Servers

Midrange to low-end servers typically cost $50,000 or less. The low-end servers would usually have one to four sockets, but with dual-core or quad core processors that are multithreaded, they are quite powerful. With the wide variety of configurations possible, these servers will be able to scale both up based on processors chosen and scale-out via cluster and mesh configurations. Typically, these servers run Linux and Windows.

The following is a technology component standard for Midrange/Low-end Servers.

Table PLA-S-09: Midrange/Low-end Servers Technology Component Standard *Updated April 04, 2011 to maintain compliance with PLA-R-37*
Strategic:
Software Windows Server 2003 family until 7/15/2015 *Microsoft Windows Server 2008 not including Hyper-V Microsoft* *Windows Server 2008 R2* Unix (Solaris, AIX, HP-UX and Linux) Virtual Server OSs (e.g., VMware and zVM; *Xen Virtual Hypervisor*) Examples Windows Server 2003*/2008 and Exchange 2007 servers* are especially appropriate for shared utility services including domain controller, file, print, email, etc. Linux may be an alternative for Web, database, and shared utility services Virtual servers and virtual machines aid in providing test environment setup Hardware Numerous manufacturers compete for low to midrange server hardware; narrowing the variety used by the Commonwealth at a point in time is important to reducing acquisition, maintenance and support across agency solutions *Multicore processors will be used increasingly as a method of improving processing capabilities of server hardware, but without corresponding application changes to take* *advantage of multithreading and parallel processing, agencies may see application degradation rather than improvement when moved to new hardware.*
Emerging:
Transitional/Contained:
Software Virtual Server OSs (e.g., VMware hypervisor, Integrity Virtual Machines, and in some cases, Windows 2003 after 7/15/2015 (when extended support ends) Windows 2003 Virtual Server R2) enable transition strategies for multiple versions of the same OS OS10 Server as a transitional OS for aiding in the use of Windows staff for Unix work due to the Windows-like user interface instead of command line
Obsolescent/Rejected:
Software Windows 2000 *Advanced Server* family *(Extended support is presently scheduled for ending July 13, 2010)* NT Novell OSX

Consolidation Platforms

A consolidation platform is typically a single high-end platform or a large aggregation of midrange or low-end platforms.

The following are technology component standards for Consolidation Platforms.

Table PLA-S-10: **Consolidate by aggregation on midrange to high-end platforms Technology Component Standard** *Updated January 15, 2010*
Strategic:
Software Unix (HP-UX, Solaris, AIX and Linux)-- *(caution: Q3 2009 acquisition of Sun by Oracle)* z/OS Windows Consolidation Examples: Appropriate for critical application and database tiers that require exceptional scaling, speed, transaction processing, reliability, etc.) Hardware Exceptional partitioning and workload management are required for the server solution. Example platforms include but are not limited to: IBM Mainframe, IBM POWERx, Sun/Fujitsu* SPARC/UltraSPARC, Fujitsu/HP Itanium x (64) and AMD Opteron (64). *(caution: Q3 2009 acquisition of Sun by Oracle)* * *Note: Sun's Q3 2009 acquisition of Oracle may cause Su/Fujitsu's' inclusion in "Strategic" to be reevaluated*
Emerging:
Ongoing management improvements. Ongoing CPU improvements: Multicore expansion to 8, 12+ processors; wer saving design changes; thread count increases; cache increases.
Transitional/Contained:
Obsolescent/Rejected:
Software
MPE
MVS OS 390 Unisys OS2200 VMS OS/400 IBM ES9000 (9221)

Table PLA-S-11: Consolidate by Scaling Out **Technology Component Standard** *Updated April 04, 2011 to maintain compliance with PLA-R-37*
Strategic:
Software Windows Server 2003 until 7/15/2015 Windows *2008; Windows 2008 R2 Solaris** HP-UX AIX Linux Examples (Note: clustering capabilities may come from other software such as MySQL Cluster which runs on most of the above operating systems.) Clusters are appropriate for MS Exchange Server (e.g., an email farm): clustered low- end to low midrange solution on Windows Server 2003*/2008*. Appropriate as a tier for single large or mirrored databases—e.g., Oracle real application clusters (RAC) running on HP-UX, AIX, Windows or Linux. Appropriate for Web hosting: (e.g., on Windows Server 2003*/2008*, HP-UX, Solaris*, AIX or Linux) Hardware Typical solutions include farms/clusters using blades or servers in racks. Commodity servers are commonly employed. Other options are possible. * *Note: Sun's Q3 2009 acquisition of Oracle may cause Solaris' inclusion in "Strategic" to be reevaluated*
Emerging:
Transitional/Contained:
Windows 2003 after 7/15/2015 (when extended support ends)
Obsolescent/Rejected:
Software Windows NT *Windows 2000*

Table PLA-S-12: Consolidate using virtual tools Technology Component Standard *Updated January 15, 2010*
Strategic:
Software Virtual Servers (via Hypervisors, or Virtual Machine Software) zVM or VMware Permit virtual Windows, Solaris*, AIX, HP-UX, or Linux machines or servers in scale-out solutions provided via zVM or VMware Hardware Typical solutions include low-end to high-end servers whose resources are divided and shared among the virtual servers which run natively within the multiple partitions. * *Note: Sun's Q3 2009 acquisition of Oracle may cause Solaris' inclusion in "Strategic" to be reevaluated*
Emerging:
Software *Windows 2008 Hyper V (Virtual Server) (scaling issues)* Hardware Intel and others are working to improve sub-processor partitioning capabilities
Transitional/Contained:
Software *Windows Virtual Server (still lacks scalability needed for many scale-out applications)* Permit virtual servers of older versions of supported OS in transitional efforts (may have some use here)
Obsolescent/Rejected:

Shared Utility Services

Shared utility services promote centralization and common handling of networked services that are currently implemented in many different ways using different practices across the served agencies and customers.

PLA-R-20 **Standardized Utilities –** Agencies with responsibilities for providing IT infrastructure shall standardize deployment, management methods and procedures for shared utility services where possible.

PLA-R-21 **Microsoft Utilities –** Agencies with responsibilities for providing IT infrastructure shall consider Microsoft best practices as guides for standardizing Microsoft Windows services across agencies until alternative shared utility services are studied and alternative methods are put into place.

Implications:

This requirement should not be construed to mean that only Microsoft Windows solutions shall be deployed for utilities, or that only Microsoft best practices should be used. Any alternatives considered should be analyzed using Microsoft utilities and Microsoft deployment recommendations as the base service to which alternatives may be compared.

For example, the majority of web server deployments may use IIS servers and may follow Microsoft best practices for their deployment. The alternative shared utility services below may have general benefit for agencies, but should be compared in cost and benefit analyses with other in-architecture options before proceeding. Example alternative shared utility services include:

- Linux as a database OS (e.g., ESRI; Oracle RAC on Linux, MySQL clusters)
- Linux for selected utilities including web hosting running on low-end servers or in soft partitions on midrange or high-end servers
- Linux for selected business applications proven on this platform
- Apache servers on Linux instead of IIS servers on Windows

Storage Utilities

The term "storage system" encompasses the hardware, software, communications, networking, media, media controllers and management tools required to record data somewhere other than on a local PC and to index the data in a manner that allows it to be retrieved at a later time.

PLA-R-22 **Storage and Capacity Planning Data –** Agencies shall perform periodic capacity and storage planning and provide those plans when requested to the agency with responsibilities for providing their IT infrastructure. The availability of planning data will improve storage, backup and disaster recovery solutions for the Commonwealth.

PLA-R-23 **Agency Assistance for Capacity and Storage Planning –** Agencies with responsibilities for providing IT infrastructure must offer capacity planning and storage planning services to assist supported agencies in determining their present and future requirements.

PLA-R-24 Storage and Capacity Planning Scope – Agencies shall consider all of their applications when conducting capacity planning and when developing a storage plan.

PLA-R-25 **Consolidated Server Storage Planning –** Agencies with responsibilities for providing IT infrastructure that manage storage consolidation shall design consolidated storage solutions with for servers used by multiple applications within an agency, by multiple agencies, or managed as a group across agencies and applications.

PLA-R-29 **Backup Consolidation and Simplification –** Agencies with responsibilities for providing IT infrastructure shall consider the value of improved backup and recovery management, reduced backup and recovery costs, and improved backup and recovery service levels when developing storage management plans and costs. This very important benefit of server and storage consolidation must be included in cost comparisons.

PLA-R-31 **Connectivity and Consolidated Storage** – Agencies with responsibilities for providing IT infrastructure shall include

assessments of connectivity needs and options for the customer base when designing consolidated storage solutions.

Rationale:

A consolidated solution often requires added connectivity. This connectivity may both increase costs and degrade throughput. The distance to the consolidation system and the costs of connectivity may be critical factors. Solutions including iSCSI, MPLS VPNs, WAFS, blade chassis, storage virtualization, and SAS are among the tools that may be beneficial in reducing total storage costs.

PLA-R-32 **Storage Location Considerations –** Agencies with responsibilities for providing IT infrastructure when designing consolidated storage solutions must evaluate the cost- effectiveness of locally consolidated storage options for the physically co-located servers if central remote storage is cost- prohibitive.

The following is a technology component standard for Storage Systems.

Table PLA-S-13: Storage Interfaces Technology **Component Standard** *Updated January 15, 2010*
Strategic[22]:
FC—FIBRE Channel single or multimode up to 12.75 Gbps in each direction: Topologies—FC-AL (arbitrated loop), FC P2P (point to point), FC SW (switched); typically Remote FCIP) FICON SCSI 10/100/Gb Ethernet; 10/100/2Gb Ethernet iSCSI PCI Express FC-IP 10GigE SAS (Serial Attached SCSI) InfiniBand (IB)
Emerging:
FCoE (Fibre Channel over Ethernet) 10 GB Ethernet
Transitional/Contained:
10/100 Ethernet
Obsolescent/Rejected:
ESCON, 17 Mbps (Mainframe) Block/Parallel (distance limits and speed problems) 4.5 Mbps (Mainframe)

Print, Fax, Scan and Copy Devices

For networked print, fax, scan and copy services, the standardizing of hardware, software, supplies, deployment, management, and staff training all offer high potential savings when coupled with paper reduction efforts.

PLA-R-33 **Print, Fax, Scan and Copy Devices and Managing Servers –** Agencies with responsibilities for providing IT infrastructure shall manage and refresh as needed in a consistent, scheduled manner all customer-oriented input and output devices that are deployed as networked devices. These devices include document scanners, fax machines, copiers, and printers along with the servers that support them.

Email Utilities, Related Communications Utilities, and Coordination Services

Historically, communications services such as email, BlackBerrys, calendaring, scheduling, conferencing, and other communications, coordination, and personal organization services were provided by individual agencies. Sometimes, the agencies used more than one product to address the email, calendaring and related needs. Typically, with the exception of phone contracts, the decisions were not made from an enterprise-wide perspective.

[22] For example, these are 2008 high end storage connectivity solutions: The Symmetrix 8000 series provides concurrent multi-host support for a wide range of open systems and mainframe platforms and operating systems with Ultra/Ultra2 SCSI, ESCON, FICON, and Fibre Channel (FC-AL or FC-SW) interfaces. Connect storage from virtually all UNIX, Windows2000/NT, Linux, mainframe, PC LAN, and AS/400 servers. http://www.sandirect.com/product_info.php?cPath=145_152&products_id=352

PLA-R-41 **Central Email Storage and Related Electronic Document Storage Solutions –** Storage for email shall address business needs and Commonwealth and Federal document retention requirements. Examples: Virginia Public Records Act and Federal HIPAA requirements.

The following is a technology component standard for email.

Table PLA-S-16: Email Technology Component Standard *Updated April 04, 2011*
Strategic:
Microsoft Exchange Server 2007 and 2010 *Email SAAS (e.g., Google, Microsoft, Yahoo, or similar email for college students)*
Emerging:
Microsoft Exchange Server 2010 (weak value anticipated without switching to Microsoft unified communications) *3rd Party solutions for email storage management policy implementation (Microsoft is still lacking in this area; this is a crucial part of email service provision)*
Transitional/Contained:
Microsoft 32 bit Exchange Server 2003 (only new installations require and EA Exception request Microsoft Exchange Server 2000 (Extended support ends in 2011) Unsupported open source implementations *Non-Exchange for VITA served-agencies*
Obsolescent/Rejected:
Microsoft Exchange Server 5.5 and earlier

Desktop Productivity Tools

The desktop productivity tools topic addresses the following technical components:

- Office Suite
  - Word Processing
  - Spreadsheet
  - Presentation
  - E-mail Client & Calendaring
  - Personal Database
- Web Browser
- PDF Authoring and Reading
- Desktop Publishing
- Desktop Project Management
- Diagramming
- File compression

The following are requirements for desktop productivity tools.

PLA-R-11 **Minimum Productivity Software for Meeting Knowledge Worker Needs –** The Commonwealth's personal computing software architecture for new desktops and notebooks shall include: Microsoft Office, Internet Explorer, Visio Reader, and

Adobe Reader. (Note: Access is not to be included in the minimum base image for most knowledge workers.)

PLA-R-43 **Desktop Productivity Tools Version/Release Levels.** The version/release levels of all desktop productivity tools included in the base images deployed by agencies that provide infrastructure services shall have vendor or equivalent level support. This support shall include security update and hotfix support.

Office Suite

An office suite is a collection of programs intended to be used by typical knowledge workers. These programs are distributed together, have a consistent user interface and can interact with each other. Office suites can include the following types of software to meet knowledge worker needs:

- Word Processing
- Spreadsheet
- Presentation
- E-mail Client & Calendaring
- Personal Database

The following is a requirement for the Office Suite component.

PLA-R-42 **Personal Database Products –** Personal or desktop database products such as Microsoft Access, Lotus Approach, or Paradox, are considered desktop productivity tools which shall not be used as a database for multi-user applications. They may be used as a front-end for strategic technology relational databases.

Implications:

Agencies that currently have multi-user applications using personal database products as a database should plan for modifying, replacing, or eliminating the application to avoid substantial risk. A migration or replacement plan must be included as part of the Agency's IT Strategic Plan.

The following is a technology component standard for Office Suites.

Table PLA-S-17: Office Suite Technology Component Standard *Updated: April 04, 2011 to maintain compliance with PLA-R-43*
Strategic:
Microsoft Office 2010 and 2007 with appropriate service packs Word, Excel and PowerPoint Viewers (highest version evaluated and tested for the environment and earlier versions that still have Microsoft Office mainstream support) **E-mail for Colleges and Universities** Google mail, Microsoft Mail, and Yahoo Mail are strategic for those Colleges and Universities that wish to provide email for students. Considerable caution should be exercised for non- student use. **Note**: Microsoft Office includes: Word, Excel, PowerPoint and Outlook. The Professional suite version also includes Access.
Emerging:
Transitional/Contained:
Microsoft Office Professional XP (extended support ends July 12, 2011). EA Exception required only for installation on a new PC. Word, Excel and PowerPoint Viewer versions that Microsoft Office is in its extended (security hotfixes still available) support life cycle
Obsolescent/Rejected:
All Microsoft Office versions that no longer have Microsoft extended support (beyond support life cycle) Word, Excel and PowerPoint Viewer versions that no longer have Microsoft Office extended support (beyond support life cycle)

Web Browser

A web browser is an application for retrieving, presenting, and traversing information resources on the World Wide Web. Information resources may be a web page, image, video, or other piece of content and are identified by a Uniform Resource Identifier (URI). Although browsers are primarily intended to access the Internet, they can also be used to access information provided by private networks or files.

The following is a technology component standard for Web Browsers.

Table PLA-S-18: Web Browsers **Technology Component Standard** *New:* *January 15, 2010*
Strategic:
Microsoft Internet Explorer (highest version evaluated and tested for the environment and earlier versions that still have full vendor or equivalent support) Mozilla Firefox 3.0.11 or a later well-tested, non-beta version
Emerging:
Mozilla Firefox 3.5 (at time of writing) Open Source Browsers (e.g., Safari, Chrome, Opera 9.6, Opera Mini 4.2, and other Opera products)
Transitional/Contained:
All versions of Internet Explorer and Firefox that are in their extended (security hotfixes still available) support life cycle
Obsolescent/Rejected:
All versions of Internet Explorer and Firefox that are beyond their support life cycle (no longer have vendor or equivalent support)

PDF Authoring and Reading

Portable Document Format (PDF) is a file format created by Adobe Systems for document exchange. PDF is used for representing documents independently of application software, hardware, or operating system. PDF was officially released as an open standard in 2008. Commonwealth knowledge workers can use Adobe Reader to view, search, digitally sign, verify, print, and collaborate on PDF documents. Knowledge workers can use Adobe Acrobat or other approved freeware PDF Authoring solutions to create PDF documents including data collection forms.

The following is a technology component standard for PDF Authoring and Reading.

Table PLA-S-19: PDF Authoring and Reading **Technology Component Standard** *New: January 15, 2010*
Strategic:
Adobe Reader, Adobe Acrobat and plug-ins (highest version evaluated and tested for the environment and earlier versions that still have full vendor or equivalent support) Approved freeware PDF Authoring solutions: PrimoPDF, CutePDF, Bullzip PDF Printer, PDFCreator, PDF 995 (highest version evaluated and tested for the environment and earlier versions that still have full vendor or equivalent support)
Emerging:
Transitional/Contained:
All versions of Adobe Reader, Adobe Acrobat and plug-ins, and other PDF Authoring and Reading products that are in their extended (security hotfixes still available) support life cycle Non-approved PDF Authoring freeware solutions that still have full vendor or equivalent support
Obsolescent/Rejected:
All versions of Adobe Reader, Adobe Acrobat and plug-ins, and other PDF Authoring and Reading products that are beyond their support life cycle (no longer have vendor or equivalent support)

Desktop Publishing

Desktop publishing allows knowledge workers to create "what you see is what you get" (WYSIWYG) publication quality documents for both large scale publishing and for small scale local multifunction output and distribution. Historically, Commonwealth knowledge workers have used multiple desktop publishing solutions.

The following is a technology component standard for Desktop Publishing.

Table PLA-S-20: Desktop Publishing Technology Component Standard *Updated: April 04, 2011 to maintain compliance with PLA-R-43*
Strategic:
Microsoft Office Publisher (and Viewer) versions: 2007 and 2010 (included In Microsoft Office) Adobe InDesign, Adobe Acrobat and plug-ins, and QuarkXPress from Quark, Inc. (highest version evaluated and tested for the environment and earlier versions that still have full vendor or equivalent support)
Emerging:
Transitional/Contained:
All Microsoft Publisher/Office versions that are in their extended (security hotfixes still available) support life cycle All versions of Adobe InDesign, Adobe Acrobat and plug-ins, and QuarkXPress that are in their extended (security hotfixes still available) support life cycle Adobe PageMaker
Obsolescent/Rejected:
All Microsoft Publisher/Office versions that no longer have Microsoft extended support (beyond support life cycle) All versions of Adobe InDesign, Adobe PageMaker, Adobe Acrobat and plug-ins, and QuarkXPress that are beyond their support life cycle (no longer have vendor or equivalent support)

Desktop Project Management

Project management software assists project managers in developing plans, assigning resources to tasks, tracking progress, managing budgets, analyzing workloads and documentation of projects.

Microsoft Office Project (Standard and Professional) is used by many project managers in the Commonwealth as a desktop project management productivity tool.

Microsoft Office Project Server is a server based tool that stores project information in a central database that supports project management across an organization. Managers can drill down into project details and can communicate project plans and distribute task assignments to team members. The team member can communicate status and changes to project manager by using Microsoft Office Project Web Access. Project Web Access is the thin web client (installed on the desktop) for Microsoft Office Project Server that can view, analyze, and report on information as well as create project proposals and activity plans.

The following is a technology component standard for Desktop Project Management.

Table PLA-S-21: Desktop Project Management Technology Component Standard *New: January 15, 2010*
Strategic:
Microsoft Office Project Standard and Professional (highest version evaluated and tested for the environment and earlier versions that still have Microsoft mainstream support) Microsoft Office Project Web Access (highest version evaluated and tested for the environment and earlier versions that still have Microsoft mainstream support)
Emerging:
Transitional/Contained:
All Microsoft Project and Project Web Access versions that are in their extended (security hotfixes still available) support life cycle
Obsolescent/Rejected:
All Microsoft Project and Project Web Access versions that no longer have Microsoft extended support (beyond support life cycle)

Diagramming

Knowledge workers can represent visual information in the form of diagrams such as flowcharts by using a diagramming program. Such programs are usually Graphical User Interface (GUI) based and feature WYSIWYG diagram editing.

The following is a technology component standard for Diagramming.

Table PLA-S-22: Diagramming Technology Component Standard *New: January 15, 2010*
Strategic:
Microsoft Office Visio: Standard and Professional editions (highest version evaluated and tested for the environment and earlier versions that still have Microsoft mainstream support) Microsoft Visio Viewer (highest version evaluated and tested for the environment and earlier versions that still have Microsoft Office Visio mainstream support)
Emerging:
Transitional/Contained:
All Microsoft Office Visio and Visio Viewer versions that Microsoft Office Visio is in its extended (security hotfixes still available) support life cycle
Obsolescent/Rejected:
All Microsoft Office Visio and Visio Viewer versions that no longer have Microsoft Office Visio extended support (beyond support life cycle)

File Compression

Compressing or "zipping" a file is a technique that can create a considerably smaller version of the original file. Zipped (.zip) versions of large files can have a reduced file size of up to 80 percent. Many zip utilities can create a self-extracting archive. These are archives that compress and package the files as an executable (.exe) file that when "clicked" to open will extract the files to re-produce the original files. Many zip utilities also allow you to encrypt files and protect sensitive data, especially when it is sent as an e-mail attachment.

Table PLA-S-23: File Compression **Technology Component Standard** *New:* *January 15, 2010*
Strategic:
Microsoft Windows file compression (included with operating systems starting with Windows XP) WinZip when used to encrypt data exchanges
Emerging:
Transitional/Contained:
Obsolescent/Rejected:
WinZip when not used to encrypt data exchanges

Mobile Communications Use

The mobile communication use requirements support the ability for state employees to use their personal mobile communications devices to access commonwealth voice and email systems to conduct official state business. Institutions of higher education are excluded from the requirements of this technical topic, but are encouraged to consider the provisions included herein when developing their internal mobile communications use policies.

The following are requirements for the General Provisions component.

MBL-R-01 **Establishment of Provisions -** Each agency shall develop a set of provisions for agency mobile communications use. The agency provisions may be more restrictive than the provisions herein, but may not be less restrictive.

MBL-R-02 **Minimum Provisions -** The agency provisions shall include, at a minimum, the provisions outlined and discussed in the following sections.

MBL-R-03 **Cost Consideration -** Agency usage provisions shall consider the additional cost to the agency to maintain the commonwealth's electronic messaging, network access services, and mobile device management capabilities when considering allowing the use of mobile communications devices.

In order to perform commonwealth business in a secure manner while using either commonwealth owned or non-commonwealth owned mobile communications devices, the following requirements shall be met:

MBL-R-04 **Authorized User -** Mobile communications devices used to conduct state business shall to be used only by the individual(s) to whom they were issued or authorized.

MBL-R-05 **Care and Due Diligence -** Each employee authorized to use a mobile communications device to conduct the business of the commonwealth is responsible for the reasonable care and due diligence in using, handling and protecting devices that access, receive, transmit, store or manipulate commonwealth data or information. Employees shall take reasonable precautions to protect mobile communications devices assigned to them from damage, loss, theft, fraud or other misuse. Devices shall not be left in unattended personal or state vehicles.

MBL-R-06 **Safe and Courteous Operations -** Mobile communications devices shall be operated in a safe and courteous manner. They shall not be used while driving, except in cases of emergency, during which times they may only be used for voice communications. They may be used with a hands free device in limited situations, but not for prolonged conversations or in heavy and/or slow-moving traffic. Text messaging while driving is strictly prohibited under all circumstances.

MBL-R-07 **Complaisance with Related Commonwealth Policies** - All mobile communications use shall comply with other related commonwealth policies including, but not limited to, DHRM Policy: 1.75 – Use of Electronic Communications and Social Media; DHRM Policy 1.60 - Standards of Conduct; and Virginia Information Technologies Agency Information Security Policy, Standards, and Guidelines.

Commonwealth Owned Mobile Communications Device Provisions

The Mobile Communications Use team identified the following commonwealth owned mobile communications device topic-specific requirements:

MBL-R-08 **Commonwealth Owned Devices and Communication Plans -** It is the commonwealth's sole responsibility and discretion to determine, select and acquire the commonwealth owned mobile communications service plans and devices needed to satisfy the business requirements of the employees or authorized users to whom they are assigned.

MBL-R-09 **Commonwealth Security Configuration -** All commonwealth owned mobile communications devices that access commonwealth data, including email, shall be configured as to meet all commonwealth security policies/requirements

MBL-R-10 **No Expectation of Privacy -** Except where prohibited by law, employees do not have, and shall not expect, privacy while using any commonwealth-owned mobile communications device. This includes usage detail information; telephone numbers dialed and received; data transmission content and email. Additionally, the commonwealth reserves the right to use Global Positioning System (GPS) or other location-tracking functionality on all commonwealth-owned devices.

MBL-R-11 **Incidental Person Use -** Incidental personal use of commonwealth owned devices is permitted as long as it does not materially or routinely impact the cost of the service to the commonwealth. The agency shall consider the position and the job function of the user when determining incidental personal use.

Non-Commonwealth Owned Mobile Communications Device Provisions

The Mobile Communications Use team identified the following non-commonwealth owned mobile communications device topic-specific requirements:

MBL-R-12 **Non-Commonwealth Mobile Device Use -** Employees, whose agency has determined require a mobile communications device for their position, may choose, if permitted by the agency, to utilize a non-Commonwealth owned mobile communications device instead of being assigned a commonwealth owned device.

a. Non-commonwealth owned devices shall only be authorized if they are used exclusively by the agency employee or user for whom they were authorized.
b. Non-commonwealth owned devices shared between the employee and family members, or employees and other parties are not eligible for use to conduct commonwealth business.

MBL-R-13 **Non-Commonwealth Device Security Requirements -** All non-commonwealth owned mobile communications devices that access commonwealth data, including email, shall be configured as to satisfy all commonwealth security policy requirements.

MBL-R-14 **Non-Commonwealth Device Use Denial** – The commonwealth reserves the right to deny the use of any non-commonwealth owned device to conduct official business that is incapable of separating personal data from commonwealth data.

MBL-R-15 **Mobile Device Management Software** – The commonwealth reserves the right to require mobile device management software to be installed on non-commonwealth owned mobile communications devices as a prerequisite for the device being authorized for use to conduct official business.

MBL-R-16 **Public Domain -** All records relating to commonwealth business are considered to be within the public domain, even though generated on a non-commonwealth owned device. State business records are subject to review and disclosure unless the Freedom of Information Act (FOIA) permits or requires them to be withheld.

MBL-R-17 **Personal Email and Records -** Personal emails and personal call records are not public records and are not subject to review and disclosure under the Freedom of Information Act (FOIA).

MBL-R-18 **Production of Public Records on Non-Commonwealth Devices –** All employees who are authorized to use non- commonwealth owned devices to conduct official state business shall agree in writing to produce any public record required by the agency, if requested.

MBL-R-19 **Commonwealth Data Removal -** If a non-commonwealth owned device is lost/stolen or the user's employment with the state is terminated, the entire device shall be electronically "wiped clean" of all commonwealth data residing on the device.

Reimbursement for Non-Commonwealth Owned Mobile Communication Devices MBL-R-20

Agency Discretion Whether Non-Commonwealth Owned Device Is Permitted - While it is up to the employee to determine if he/she prefers to use a non-commonwealth owned device to conduct official business, it is the agency's sole

discretion, to determine whether non-commonwealth owned devices shall be allowed and the conditions under which they shall be supported.

MBL-R-21 **Reimbursement -** Reimbursements shall only be offered to employees who provide approved devices that are provisioned to support voice and data, or data-only functions (i.e., "smart" devices). Cellular telephones and other devices that only support voice and text messaging are not capable of or not configured to, at minimum, receive commonwealth email messages are not eligible for a stipend or reimbursement.

MBL-R-22 **Stipend Restriction -** Employees or authorized users shall normally only be authorized a single stipend for single non- commonwealth owned mobile communications device. Exceptions to this provision may be granted by the agency head (or designee). Documentation of the exception and its justification shall be retained in the agency's files for the duration the exception is in effect.

Department of Accounts Requirements

The Department of Accounts (DOA) has established provisions in the Commonwealth Accounting Policies and Procedures (CAPP) Manual that govern the terms under which agencies may provide stipends to employees as reimbursements for the use of non- commonwealth owned mobile communications devices to conduct official business. See CAPP Manual, Volume 1 – Policies and Procedures, Topic: 50535, Mobile Device Provisions.

MBL-R-23 **Maximum Allowed Reimbursement -** The DOA policy establishes the maximum allowed reimbursement and how it shall be applied in order for the stipend to be provided in compliance with commonwealth policies and federal Internal Revenue Service (IRS) income tax and withholding laws. The current maximum allowed reimbursement is $45.00 per month.

MBL-R-24 **COV Mobile Device Allowance Agreement -** The DOA policy requires that prior to providing a stipend to an employee who is authorized to use a non-commonwealth owned mobile communications device, the employee's supervisor and the agency head (or designee) shall sign the "COV Mobile Device Allowance Agreement". The agreement form can be found at: http://www.doa.virginia.gov/DOA/DOA_Forms_Alpha.cfm

Agency Mobile Communication Use Policies

MBL-R-25 **Mobile Communications Use Policy -** Each agency shall develop an agency mobile communications use policy. The agency policy may be more restrictive than the requirements provided herein, but may not be less restrictive. The agency policy shall include the general use provisions above and, at a minimum, the provisions outlined and discussed in the following sections.

MBL-R-26 **Mobile Communications Device Use Justification -** Each agency shall be responsible for determining the criteria for which positions in that agency require the provision of a mobile communications device and the type of service. Provision of a mobile communications device shall be limited to those positions requiring the device for a specific job function (e.g., public health, welfare and safety), to improve customer service or for a proportional increase in productivity justifying the cost.

MBL-R-27 **Single Mobile Communications Device Limitation -** An employee shall not be authorized more than a single mobile communications device, unless an exception is documented and approved by the agency head (or designee).

MBL-R-28 **Mobile Communications Device Use Criteria -** The criteria for providing a mobile communications device shall include, but is not limited to, the following considerations:

a. A requirement to travel frequently on commonwealth business.
b. Considerable amounts of time spent away from the office.
c. A need for customers to be in constant communication with the individual.
d. A need for the individual to be constantly available while out of the office.
e. Personal safety concerns for individuals while working.
f. A need to contact the individual after normal business hours on a consistent basis.

MBL-R-29 **Identification of Positions Meeting Mobile Communications Device Use Criteria -** The agency shall clearly identify and document which positions in their agency meet the defined criteria. Positions with similar job functions or needs shall be grouped together with the same justification. The goal is to clearly identify those positions within the agency requiring a mobile communications device

- As an example, the agency policy could state that all agency employees meeting with customers outside the office require a mobile communications device for personal safety.
- A list of the specific job titles meeting this criterion shall also be included (i.e. Case Manager, Site Inspector, etc.).

MBL-R-30 **Service Type -** In addition to defining which positions require a mobile communications device, the type of service provided to the position shall be identified. Many different types of service are available at a wide difference in cost. Since one of the goals of this policy is to be cost effective, the least expensive device and service that meet the agency's business requirement shall be identified for each position.

a. The most basic service would provide only a voice capability to the user. Advanced services can provide access to commonwealth email and many other applications. The type

of service required shall greatly depend on the requirement of the position.

b. Care shall be taken to ensure the correct plan of included minutes is identified. Overages of those minutes can be costly. Routinely using less than the allowable minutes can also be costly.
c. Actual usage shall be monitored and plans managed to ensure the most cost effective service plans are utilized.
d. As an example, if the requirement is for personal safety a voice-only device and service will likely meet the requirement.
e. If there is a requirement to be accessible by email when out of the office, then a Blackberry or smart phone and data service shall be required at an additional cost for both the device and the monthly service.

MBL-R-31 **Service Plan Level -** The level of service plan shall be identified. Though the level of service plan varies among the mobile service providers, consideration shall be given to the level of service required for each position.

a. Care shall be taken to ensure the correct plan of included minutes is identified. Overages of those minutes can be costly. Routinely using less than the allowable minutes can also be costly.
b. Actual usage shall be monitored and plans managed to ensure the most cost effective service plans are utilized.

Rationale

- As a general rule, a pooled minute service plan is the most cost effective service plan for an agency. With a pooled minute service plan, the agency pays a low fixed cost for each device and those devices share a large pool of minutes for voice telephone calls.
- The alternative is an individual plan where the included minutes for voice calls are defined for each device.

MBL-R-32 **Determining Factors for Non-Commonwealth Owned Devices -** Each agency shall determine if non-commonwealth owned devices will be permitted for those employees requiring mobile communications devices. Factors impacting this decision shall include the function of the device.

Rationale

- Some devices can easily be used for simple voice calls and email access, but may not be appropriate for running mobile applications due to resource and configuration limitations on the personal device.
- Some mobile applications require specific operating systems, memory/processor requirements or other application specific configurations.
- Managing and testing the varied device configurations would likely prove too costly and inefficient to justify their support. As a result, the agency

may prohibit non-commonwealth owned devices from use on the commonwealth network.

MBL-R-33 **Agency Responsibility for Non-Commonwealth Owned Devices -** Agencies, at their sole discretion, shall elect to provide a stipend to reimburse employees authorized to use smart non- commonwealth owned devices for commonwealth business. There are costs to the agency if the device accesses the employee's commonwealth email account or network resources. The agency is still responsible for the cost of these services even for non-commonwealth owned devices.

a. The option of using a non-commonwealth owned device is provided solely for the convenience of the employee so as not to require two mobile communications devices to be carried (one personal and one business).
b. While it is up to the employee to determine if they prefer to use a non-commonwealth owned device, the agency shall first determine if they will support that option.
c. Stipends shall only be offered to employees who provide approved non-commonwealth owned devices that are provisioned to support voice and data, or data-only functions (i.e., "smart" devices).
d. Agencies shall not offer a stipend that exceeds the monthly amount authorized under this policy. The current maximum allowable monthly stipend is $45.00. Stipends paid to employees who are authorized to use non-commonwealth owned devices are not considered part of the employee's compensation and are not subject to federal or state income taxes.
e. Agencies shall not offer a stipend or reimbursement to an employee or authorized user who has been assigned a commonwealth owned mobile device, but has also been authorized to use a non-commonwealth owned device.

MBL-R-34 **Non-Commonwealth Owned Use Agreement -** If non- commonwealth owned devices shall be permitted, the agency mobile communications policy shall include an "Non- Commonwealth Owned Use Agreement" that defines the requirements placed on the employee and grants the commonwealth management of the non-commonwealth owned device, as required, depending on the capabilities of the non- commonwealth owned device.

Management of Mobile Communications

MBL-R-35 **Processes to Minimize Cost -** The agency mobile communications use policy shall establish processes to manage and monitor the use of mobile communications devices for purposes of minimizing costs and eliminating unauthorized use.

a. This shall be accomplished through evaluation of detailed billing for each device, as appropriate, or shall be provided

through a periodic review conducted by a Telecommunications Expense Management (TEM) firm.

b. Internal review processes shall also be established to ensure compliance with the agency policy, including periodic assessments of ongoing individual and agency-wide business justification and plan usage effectiveness.

MBL-R-36 **Device Inventory -** The agency mobile communications use policy shall establish a process to maintain a current inventory of the wireless devices used by the agency. At a minimum, the inventory shall include a description of each device, the service provider for each device and the individual to whom the device is issued.

MBL-R-37 **On Boarding and Off Boarding -** The agency mobile communications use policy shall specifically detail the on-boarding and off-boarding processes.

a. The on-boarding process shall include the review and approval process for initiating service as well as a requirement for the employee to read and to acknowledge awareness and acceptance of the agency and statewide policies. This acknowledgement shall be in writing and include provisions for the agency to withhold the value of the commonwealth owned device from the employee's pay if it is not returned upon request or termination.
b. The off-boarding process shall include the recovery of any commonwealth owned devices from the departing employee, the cancellation of services, removal of information from the device and the storage or disposal of the device.
c. The off-boarding process shall include the timely removal or wiping of all commonwealth data and information from the non-commonwealth owned mobile device of the departing employee.

Special Security Consideration

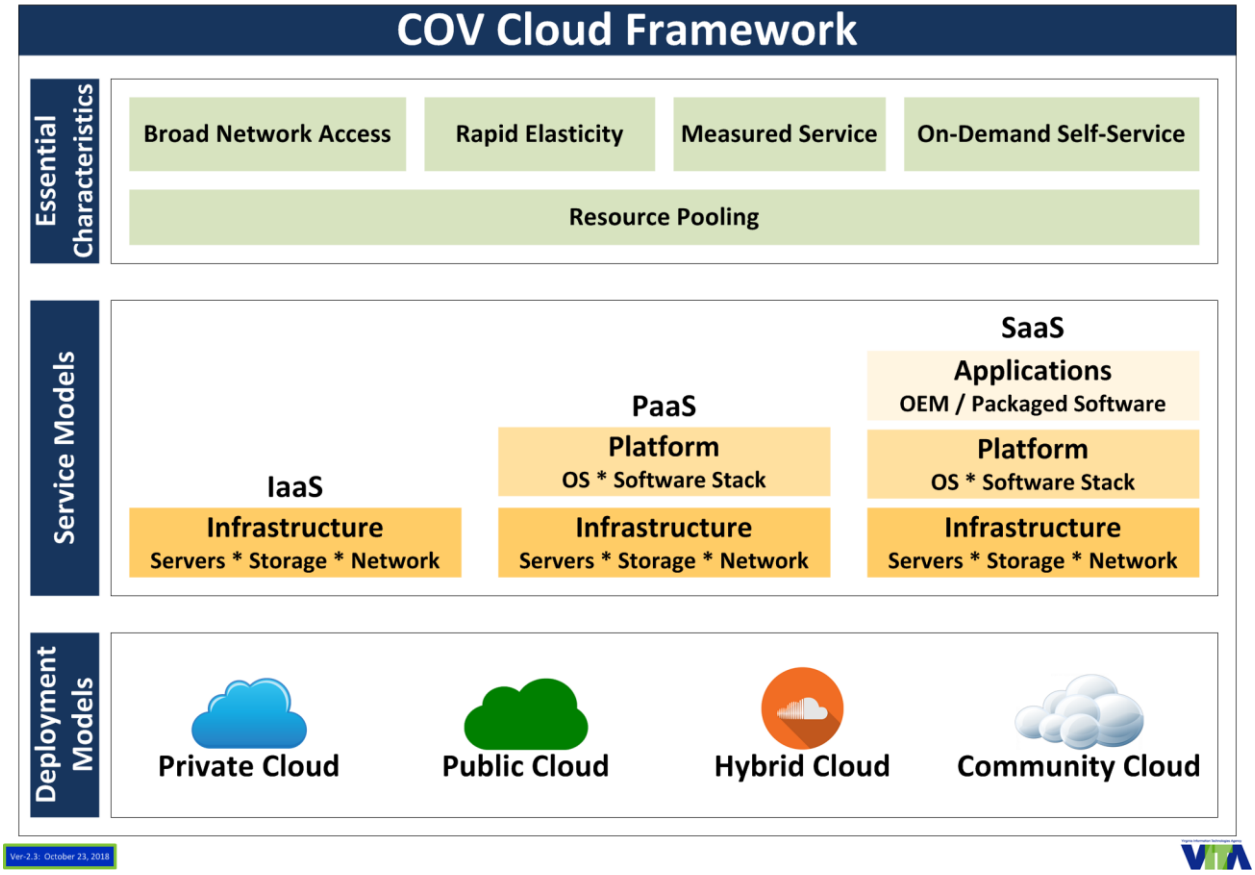
MBL-R-38 **Special Security Considerations** - The agency mobile communications use policy shall clearly identify any special security considerations for mobile communication devices. This shall include any prohibitions for accessing agency data or resources from the mobile device.

a. It shall also include any features of the mobile device that shall not be used even if available through the service plan.
b. Some features such as text messaging do not create a record that can be maintained if they are used for conducting commonwealth business.
c. Employees may be required to use email to ensure that a record is created though text messaging may be more convenient.

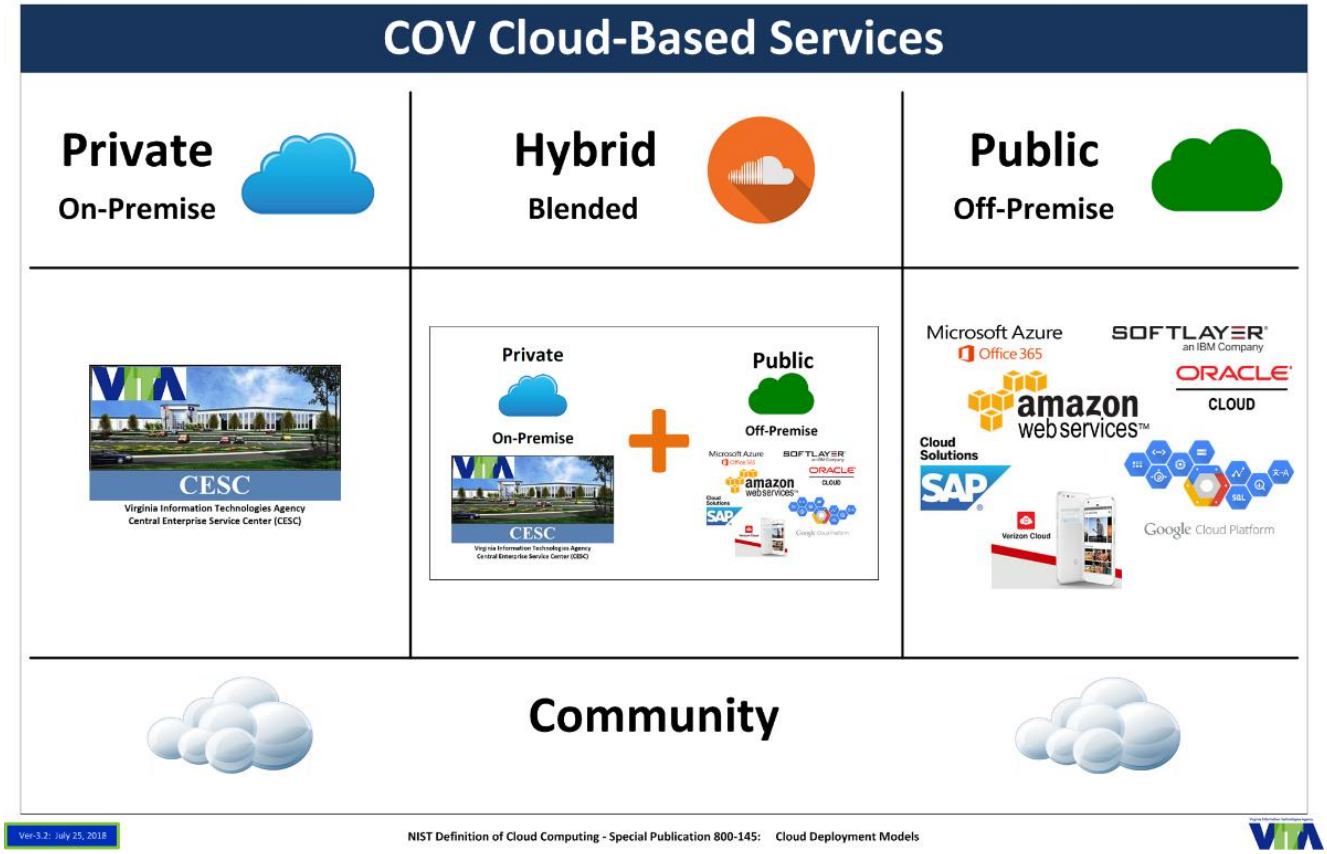
Cloud-based Hosting Services

Objective 1: Framework

CBH-R-01: **Define the cloud-based hosting services within the framework –** COV cloud-based services shall cover all COV defined services and deployment models, will meet all five of the characteristics and will be deployed both on premise and off-premise as follows:



Cloud computing is 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) that can be rapidly provisioned and released with minimal management effort or service provider interaction.



Objective 2: Services

CBH-R-02: **COV Cloud-based hosting service models –** the commonwealth COV cloud-based services models shall include Platform as a Service (PaaS) and Software as a Service (SaaS) service models.

CBH-R-03: **COV cloud-based hosting services –** cloud-based hosting services shall conform to the following five essential cloud characteristics: on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service.

CBH-R-04: **Commonwealth data concerns –** cloud-based service suppliers and the CSB shall document and provide the answers to the following questions for all cloud-based services that host commonwealth data:

- Who owns the data?
- Where is the data located?
- How does the commonwealth get the data back?
- How does the commonwealth confirm the data is deleted?
- How is the data secured?
- How does the commonwealth confirm that the data is secure?

CBH-R-05: **Proposed service cost modeling and service use cost estimation modeling –** COV cloud-based hosting services shall include the functionality to allow customers to:

- Compare costs for hosting their IT solution among the proposed deployment and service models
- Project spending on hosting services

CBH-R-06: **Cloud-based service integration model –** Cloud services will be offered through a Cloud Service Broker (CSB) integration model. All enterprise cloud services shall integrate any existing and future cloud-based hosting services into the CSB model. The CSB shall at a minimum include the following features:

- Provide an extended hybrid cloud management tool
- Provide new service onboarding
- Integrate with the VITA service catalog/app store
- Provide cost modeling
- Provide cost monitoring (expenditures vs. budgeted)
- Connect CSB applications to single sign-on services for end users
- Support end-to-end monitoring
- Provide unified billing and reporting
- Report performance and utilization information
- Integrate and enforce commonwealth's governance requirements

CBH-R-07: **Cloud-based hosting service contracts –** the Cloud Service Broker (CSB) shall ensure that the commonwealth and its customers have the provision to "get out" of a cloud-based hosting contract if needed/required.

CBH-R-08: **Cloud-based hosting services support of containers –** the COV hybrid cloud-based hosting services shall include support of containers.

Objective 3: Suppliers

For VITA supported agencies, the cloud-based hosting supplier services have been procured as part of the Infrastructure Sourcing efforts. These contracts can be found at the VITA Supply Chain Management (SCM) Statewide Contract Search webpage: https://vita.cobblestonesystems.com/public/.

CBH-R-09: **Compliance to COV cloud framework characteristics** – suppliers shall document how the deployment models for their services comply with COV cloud framework characteristics.

CBH-R-10: **Customer access to support –** suppliers shall provide access to technical support for all customers (localities and executive branch agencies).

CBH-R-11: **Pricing transparency –** suppliers pricing (including estimation models) shall be transparent, accessible and integrated with the Commonwealth CSB.

CBH-R-12: **Remove barriers for consuming on-premise cloud-based hosting services –** suppliers of on-premise private cloud-based hosting services shall remove technical and financial barriers to the use of those services. This includes supporting enough cores, memory, storage, bandwidth, connectivity, throughput, and any other capability needed to support the vast majority of agency applications including their associated databases.

CBH-R-13: **Deployment technology stack with PaaS –** cloud-based hosting service suppliers shall follow an approach of providing services that include as much of the deployment technology stack required by IT solutions into PaaS as appropriate. This means the components of the deployment technology stack (database, application server, monitoring tool, etc.) should be included in PaaS services.

Objective 4: Customers

The procurement and deployment decisions on IT solutions impact both the possible service and

deployment models available and those options drive cost. For this reason, additional effort must be spent by the agencies to drive these decisions. Enabling the ability to consume additional hosting choices means the information driving service and deployment model decisions must be captured as early in the procurement process as possible.

CBH-R-14: **Application succession plan –** all IT solutions hosted off-premise shall have a plan for what could be done if circumstances arise that require the solution to be moved or migrated (what happens if the hosting entity fails, has a breach, etc.).

- This plan must be reviewed and updated as part of customer governance whenever significant changes occur to the solution, deployment, or data
- Examples of plan options to consider:
  - Can the SaaS solution migrate to another host? Optimally, there would be multiple SaaS vendors on contract and other agencies also using that same SaaS solution (this minimized risk which should be evaluated as part of the governance process)
  - Can the customer migrate to another SaaS solution (data needs to able to be exported and then imported)?
  - As a last resort, can the solution be brought back in house? Are the technologies needed strategic? (supported by VITA and partners)

CBH-R-15: **Assess IT solutions for cloud readiness –** all IT solutions shall be assessed for cloud readiness.

CBH-R-16: **Assess new IT solutions for cloud readiness –** all new IT solutions shall be assessed for cloud readiness as part of the procurement process.

CBH-R-17: **New IT solution hosting –** all new cloud ready IT solutions shall be hosted by cloud-based services (private, community, and/or public).

CBH-R-18: **IT Strategic Plan –** agencies/customers shall include in their IT Strategic Plans efforts to migrate to cloud-based services and other determined future states.

CBH-R-19: **SaaS vs. PaaS –** agencies/customers shall follow a tactical approach of utilizing SaaS over PaaS for back office functions and as appropriate for core business functions.

Cloud readiness

CBH-R-20: **Pursue cloud readiness –** agencies shall ensure that all new IT solutions are cloud ready and agencies shall also have a plan in place to maximize the potential of their current solutions to be cloud ready. New IT solutions are defined as solutions that are not implemented or do not have an approved strategic plan entry as of 10/1/2018.

CBH-R-21: **Cloud readiness requirements –** VITA shall create a tool that will use the defined cloud readiness attributes to establish the cloud readiness of current or proposed agency/customer IT solutions

CBH-R-22: **Support for becoming cloud ready –** VITA shall ensure that there are adequate supplier choices and resources available to assist agencies/customers in assessing cloud readiness or for migrating existing IT solutions to cloud-based hosting services. Suppliers for these resources will include:

- CAI contract,
- CSB,
- Infrastructure server services suppliers, and
- Cloud-based hosting suppliers.

CBH-R-23: **Cloud readiness assessment –** agencies shall complete the VITA cloud readiness assessment instruments, and VITA with the agencies will identify which of the following six cloud readiness determinations best fit each IT solution:

1. **Already hosted on cloud-based services –** IT solution has achieved the desired future (to-be) state for consumption of cloud-based services
2. **Cloud ready**

   Preferred – IT solution is hosted on a virtual x86 or equivalent server using either Linux or Windows as an operating system and there are no software licensing or data issues with the solution consuming cloud-based hosting services. This also includes any IT solution under ECOS evaluation.

   Acceptable – IT solution is hosted on a non Windows/Linux virtual machine (examples: AIX, Solaris) that could be hosted by either a private cloud or by a community/public cloud provider where there are no software licensing or data issues with the solution consuming those cloud-based hosting services.
3. **Not currently cloud ready and cannot be made ready –** IT solution is not currently cloud ready and it may or may not be possible for it to become cloud ready
4. **Not currently cloud ready, can be and should be made cloud ready –** the IT solution can technically be made cloud ready and there is a business case for doing so
5. **Not currently cloud ready, can be but should not be made cloud ready –** the IT solution can technically be made cloud ready and there is not a business case for doing so
6. **Does not apply –** PC deployed IT solution that included no server-based components

CBH-R-24: **Agency business cases for cloud migration –** agencies shall develop business cases that will be used to determine if current IT solutions that can be made cloud ready should be migrated to cloud-based services.

CBH-R-25: **Software Licensing Requirements –** agencies shall know all of the software licensing requirements for the two technology stacks needed for each of the IT solutions under consideration. For each technology stack component, agencies should know:

- Name of software component and vendor
- Type of licenses needed (site, instance, CPU, core, named user, concurrent, etc.)
- If the license supports virtual servers
- If the license supports cloud deployment
- It is suggested that the agencies also know: the number of licenses; who owns/provides the licenses; pricing options; and renewal schedule

Objective 5: Governance

The commonwealth's intent is to ensure that agencies/customers do not compromise their business by trading the confidentiality, integrity, and availability of critical data and information in pursuit of the benefits cloud-based hosting services may offer. The potential IT solution vulnerabilities and impacts to business operations must be carefully and continuously assessed, then weighed against the advantages of adopting cloud-based hosting services for agency/customer IT solutions.

CBH-R-26: **Compliance to COV ITRM Policies and Standards –** supplier's cloud-based services shall comply to COV ITRM policies and standards.

CBH-R-27: **All new cloud ready IT solutions –** shall either be hosted by hybrid cloud-based

services (private, community, and/or public) or will have a documented business rationale for not using those services.

CBH-R-28: **VITA Supply Chain Management (SCM) –** shall be engaged and involved in any procurement of any cloud-based hosting services.

CBH-R-29: **Virtual vs. physical servers –** New traditional hosted solutions shall be hosted on virtual servers. Use of physical servers will require an approved EA exception.

CBH-R-30: **Service and deployment model review –** processes shall be created and implemented to enable IT solution owners to select an appropriate Service Model (PaaS, or SaaS) and Deployment Service Model.

CBH-R-31: **Governance processes for Software as a Service (SaaS) –** all requests for consumption of SaaS cloud-based hosting service must be submitted for review and approval via the ECOS process.

CBH-R-32: **Governance for Platform as a Service (PaaS) –** agencies shall only consume VITA provided PaaS cloud-based hosting services.

CBH-R-33: **Architectural review –** all changes to solutions, hosting services, and choices of deployment models shall go through a formal review process. This process should have a customer internal component and if needed due to technical complexity, an integration with an external review performed by the MSI/CSB. The reviews must take a multidisciplinary approach. It is suggested that customer's internal review team include roles when appropriate of: Business Owner, Technical Owner, Security Owner, and Data Owner.

CBH-R-34: **Governance for Platform as a Service (PaaS) –** agencies shall review all of their IT solutions annually to ensure that the solution is consuming the appropriate hosting service.

Section 5.7 - ETA Security Domain

The Security Standards are available on the VITA website. The current versions of the following documents are ITRM Security Standards for state executive branch agencies.[23]

- Information Technology Security Audit Standard (SEC502)
- Information Technology Security Standard (SEC501)
- Information Technology Standard: Use of Non-Commonwealth Computing Devices to Telework (SEC511)
- Removal of Commonwealth Data from Surplus Computer Hard Drives and Electronic Media Standard (SEC514)

[23] The security documents can be found here: http://vita.virginia.gov/library/default.aspx?id=537#securityPSGs

Section 5.8 - ETA Enterprise Systems Management Domain

The ETA Enterprise Systems Management (ESM) Domain defines the operational aspects of IT services delivery and identifies generally accepted industry policies, practices, standards, and processes for administering, monitoring, and controlling hardware and software components of the infrastructure.

ESM activities include but are not limited to, network monitoring, monitoring servers, applications monitoring, net-flow analyzer, troubleshooting tools, helpdesk, assets management, storage management, wireless LAN management, event management, and performance management.

ESM processes focus on methods, techniques and procedures relating to IT service management (configuration management, event and state management, fault detection and isolation, performance measurement, patch management, vendor relationship management including Service Level Agreements (SLA), release management, change control, problem reporting, and hardware and software retirement).

ESM addresses three major topics, Service Delivery, Service Support, and Operations Management. The Service Support topic is further sub-divided into Supporting and Changing sub-topics.

Domain-wide Requirements

The following domain-wide requirements pertain to all topics and components in the Enterprise Systems Management Domain.

ESM-R-01 **Authorized Access –** Agencies shall restrict access to any IT infrastructure resources including ESM tools in conformance with the Commonwealth's security policies and procedures.

ESM-R-02 **Adhere to Information Technology Infrastructure Library Framework (ITIL) –** IT operational and services processes shall adhere to the ITIL framework best practices methodology.

ESM-R-03 **Security, Confidentiality, Privacy, and Statutes –** IT systems shall adhere to all security, confidentiality and privacy policies, and applicable statutes.

ESM-R-23 **Components of Services Provided –** Providers of enterprise services shall adopt and publish operational standards that are required to manage, control, support, and monitor infrastructure components supporting the services that they provide. The published operational standards are considered mandatory components of the services provided to customers.

ESM operational standards related to services received through VITA are published on the VITA website under VITA Services

Service Delivery

Service Delivery relates to managerial and procedural activities that operations management must support to meet customers' business requirements. The management actions and activities associated with this core process are planning, administration, cost control, service options catalog, and customers' service management.

ESM-R-04 **Service Level Agreement -** Agencies shall ensure that service delivery expectations are defined and documented in a Service Level Agreement (SLA). The SLA must include performance requirements and methods for measuring IT service delivery against performance targets.

ESM-R-05 **Capacity Planning and Performance Monitoring Management -** Agencies with ESM responsibilities shall perform capacity planning and performance monitoring to ensure infrastructure resources are appropriately sized to meet current and planned workload demands.

ESM-R-06 **Financial Management for IT Service Management -** Agencies with ESM responsibilities shall implement accounting processes and procedures that identify and attribute costs for IT resources used to support the business processes. The process shall provide data in a timely manner for Total Cost of Ownership (TCO) analysis and reporting.

ESM-R-07 **IT Continuity Management -** Agencies with ESM responsibilities shall establish an IT disaster recovery plan that reflects SLA service delivery requirements. This risk-based plan shall incorporate the operating constraints of the business continuity plan. The plan shall address all critical applications, middleware, operating systems, hardware, and network connectivity elements. In addition, there shall be procedures to test the IT disaster recovery plan periodically and update the plan based on the test outcome or environment changes.

Service Support

Service Support is the connection between the other core processes. The primary role for Service Support is to be the communication channel between the customer and the IT service organization. There are two sub-processes, Supporting and Changing, by which customer's interactions take place. It is through these sub-processes that IT service personnel handle all customer-facing issues and problems.

Supporting

The *Supporting* sub-topic is a set of process capabilities that are directly related to customer interactions with the IT service organization. Customer interactions can include reporting of problems and incidents, requests for service; and obtaining information about service events, actions, and opportunities that could improve individual productivity. The Service Desk is the single point of contact for all customer communications, tracking of customer contacts, and maintenance of a repository of customer data.

ESM-R-08 **Service Desk -** Agencies shall utilize a Service Desk facility that is staffed with properly trained personnel who can minimally respond to level 1- type problems, incidents, and events[24]. The Service Desk shall utilize an automated contact management tool and is the single point of contact for all IT service requests and services communications.

ESM-R-09 **Incident Management[25] -** Agencies with ESM responsibilities shall establish an Incident Management process and procedures. The process and procedures shall enable restoration of normal service operation as quickly as possible and minimize the impact on business operations. Procedures shall include steps to address actions such as incident detection, recording, classification, initial support, investigation, diagnosis, resolution, recovery, closure, ownership, monitoring, tracking, and communication.

ESM-R-10 **Problem Management[26] -** Agencies with ESM responsibilities shall institute procedures for problem handling. These procedures shall include steps for performing root cause analysis of incidents and correction of the error to the satisfaction of the customer.

Changing

The *Changing* sub-topic is a set of process capabilities that ensure standardized methods and procedures are used for efficient and prompt handling of all changes, releases, and configuration actions in order to minimize the impact on service quality commitments, and consequently improve the day-to-day operations of the IT organization.

ESM-R-11 **Change Management -** Agencies with ESM responsibilities shall establish a Change Management process and institute procedures that provide for the analysis, implementation, and follow up of all environmental changes requested including those made due to problem resolution. The process shall support change initiation and control actions, support the ability to conduct impact assessments, handle changes in an automated manner including emergencies, document all changes in the configuration management database, demonstrate chain of custody for the change, and comply with release policies.

ESM-R-12 **Release Management –** Agencies shall establish a release management process. Process activities shall include procedures for hardware, license/version control across the infrastructure, rollout planning, communication protocols, and quality control of the process.

ESM-R-13 **Configuration Management -** Agencies with ESM responsibilities shall establish a cost effective automated Configuration

[24] Level 1-type problems, incidents, and events are user calls to the service desk that the service desk analyst can resolve directly with the user using prior experience and/or information accessed from a knowledge base.
[25] An incident is any event which is not part of the standard operation of a service and which causes, or may cause, an interruption to, or a reduction in, the quality of that service.
[26] A problem is a condition resulting from multiple incidents or a significant incident for which the cause is unknown but the impact is significant. Problem Management's purpose is the detection, resolution, and prevention of future incidents.

Management process and procedures to control and identify all IT assets[27] (Configuration Item [CI]) and their physical locations. CIs must be documented in a Configuration Management Database (CMDB)[28]. The CMDB shall have the ability to create a parts list of every CI in the system, define the relationship of CIs in the system, track the current and historical status of each CI, track all Requests for Change (RFC) to the system, and verify that the CI parts list is correct and complete.

Operations Management

Operations Management is responsible for the day-to-day administration of all infrastructure components. Key tasks associated with this core process are highly technical in nature. They include installation; repairs; maintenance; jobs management; performance monitoring and data capture for reporting; and fault management to name a few. Operations Management, therefore, complements the Service Delivery process.

Operations Management includes Security Administration, Network Administration, Storage Management, Systems Administration, Services Monitoring and Control, Directory Services Administration, and Job Scheduling.

Service Monitoring and Control

Service Monitoring and control consists of procedures and tools for proactive notification of events that may have severe consequences on the business. In addition, to the extent performance metrics are defined, monitoring of these metrics is important for SLA management and reporting.

ESM-R-14 **Metrics -** Agencies with ESM responsibilities shall implement operational performance metrics, data collection processes, and conduct regular reviews to ensure performance targets are on track and variations are addressed in a timely manner.

ESM-R-15 **Monitoring Capability -** Agencies with ESM responsibilities shall establish a system event monitoring console and institute systems performance alert thresholds to ensure systems faults are averted and corrective measures are taken to limit the chance of total systems failure.

ESM-R-16 **Monitoring and Control Tools -** Agencies with ESM responsibilities shall use Commercial–off– the Shelf (COTS) ESM tools that meet the goals of the International Standards Organization (ISO) 20000[29] and support performance metrics

[27] ITIL framework use the "lowest common denominator" principle for IT asset management. Configuration item is the term used to describe all components necessary for IT operations. Configuration Management activities include: (1) planning, (2) identification, (3) control, (4) status accounting, and (5) verification and audit. Any configuration item therefore is considered as an IT asset thus IT asset management is not treated as a separate function but instead handled as an integral part of the Configuration Management process.

[28] Many vendors' product offerings view CMDB as the most important repository within ESM. While non-automated methods are an option, it is not a recommended practice. ESM tools that have the ability to perform "auto discovery" to capture, record, track, define relationships, and handle changes etc are the preferred option. Use of manual procedures will over time lose its usefulness and could become cost prohibitive.

[29] International Standard Organization (ISO) 20000 (which replaces BS15000) defines the requirements for an IT Service Management System. It sets out the main processes to deliver IT services effectively. The standard supports all aspects of ITIL. Details for ISO 20000 can be accessed at http://20000.fwtk.org/iso-20000.htm

agreed to in SLAs. In the case where internally developed ESM tools[30] provide the best course of action, the tool shall comply with the ITIL process and appropriate dedicated staff resources(s) shall be assigned on a continuous basis to provide ongoing maintenance and updates.

ESM-R-17 **Network Administration -** Agencies with ESM responsibilities shall ensure that critical networking infrastructure devices such as routers, switches, hubs, PBX/call manager, voice mail server, and other direct attached data communications devices are Simple Network Monitoring Protocol (SNMP) capable. Devices shall be configured to capture of all events required by the SLA and the captured data shall be stored in a Management Information Base (MIB) repository. Procedures shall be integrated with the Service Monitoring and Control process.

Storage Management

The Commonwealth data is vital to providing citizen services. Exercising strict data management controls necessitates having operating processes and procedures that ensure that the data is protected, retrievable, and recovered in a timely manner to meet business continuity requirements. Storage Management is concerned with data custody and control of the environment. Storage Management operational process consists of two major focus areas: (1) Data Backup, Restore, and Recovery Operations and (2) Storage Resource Management.

ESM-R-18 **Policies and Procedures –** Agencies with ESM responsibilities shall establish data storage and archival retention policies and procedures that meet operating business requirements, statute, and regulatory mandates. To the extent there are conflicting requirements, agencies shall address all conflicts with the appropriate mandating entity and document the resolution.

ESM-R-19 **Back-up and Recovery –** Agencies with ESM responsibilities shall ensure policies and procedures address back-up and recovery for all critical Commonwealth data and conduct testing of these procedures on a regular basis. Procedures shall address timing, frequency, and restore time objectives (RTO) that support the business continuity plan.

ESM-R-20 **Off-Site Retention –** Agencies with ESM responsibilities shall ensure critical back-up data files are rotated to an Off-Site location on a scheduled basis as defined in the back-up and recovery procedures. In addition, Off-Site locations shall comply with data security requirements as defined in the ETA security domain.

ESM-R-21 **Systems Administration -** Agencies with ESM responsibilities shall develop and maintain appropriate operations policies, procedures, and standards to ensure day-to-day management of the IT infrastructure environment. Developed policies, procedures,

[30] Internally developed tools shall be engineered using Systems Development Life cycle (SDLC) methodology that complies with the Commonwealth's software development policy and standards.

and standards shall comply with applicable ETA policies and standards.

ESM-R-22 **Job Scheduling -** Agencies with ESM responsibilities shall utilize an automated job scheduling system to control and organize workloads. Features shall include, but are not limited to, parameters for execution time periods (daily, weekly, monthly, annually), execution length (start/finish), storage requirements, dependencies, and the ability to limit job execution bypass.

Technology for Enterprise Systems Management

Specific enterprise systems management tools are not addressed in this release of the ETA Standard. Future updates to this standard may address specific tool sets that support the requirements in this standard.