ATTACHMENT G: ENTERPRISE ARCHITECTURE INTERGRATION REQUIREMENTS FOR ENTERPRISE/STATEWIDE SYSTEMS – REVISED 6/21/2021

Louisiana Office of Technology Services

Technology Overview

The State has made a significant investment in a hardware and software platform to form the foundation for development and hosting of statewide enterprise systems. The Enterprise Architecture (EA) platform consists of eight core components hosted on a hyper converged infrastructure spanning two State-owned data centers in an active-active configuration. This highly available platform (99.99% uptime) should be utilized for all enterprise or mission critical applications. The State has employed the core concepts of the software defined data center (SDDC); converging storage, networking, and compute resources into a single lifecycle model.

The platform is monitored through the coordinated use of the following tools: infrastructure and network monitoring, application performance monitoring (APM), security information and event management (SIEM), and log aggregation. This suite of tools allows the State to track and monitor the overall health and operation of the platform and to quickly respond to performance demands. A significant investment has been made in a DevOps approach and tooling including IT build and deployment automation.

In addition to the EA platform, the EA initiative provides for standardization of other areas of the software development lifecycle (SDLC). The State provides tools for project management, requirements definition, risks, issues, and other project documentation and artifacts. Contractors must use these State provided tools as part of the project management lifecycle.

Key Goals

1. The consuming application platform is irrelevant to the use of the EA component except in the methodology used to integrate. State standards require custom built, transfer, or non-COTS/SaaS systems to be developed in C#/.Net although other integrations may exist.
2. All applications or systems integrating into the EA platform must integrate into these components using standard SOAP/REST APIs or connectors or message queues within the ESB or APIGW.
3. All applications or systems integrating into the EA platform must integrate with the Identity Access Management /Single Sign On, API Gateway, and/or Enterprise Service Bus components, irrespective of which of the other components will be used.
4. All integrations must be reviewed and approved through the State's governance processes.

Operations and Governance

The Enterprise Architecture is designed upon the Information Technology Information Library (ITIL) and The Open Group Architectural Framework (TOGAF) frameworks. Integrating solutions shall adhere to the State's Enterprise Architecture Governance processes to include:

- **Change and Release Management**

    - Changes to Production must be submitted to the State's EA Change Control Board (CCB) for evaluation
- **Performance Management**
    - Monitor and Report on Key Performance Indicators in accordance with Industry Best Practices
    - Real-time Business and IT dashboards will be published
    - Integrating systems shall define uptime and performance SLAs as part of any resulting contract
- **Incident and Problem Management**
    - Any event that results in the violation of a Service Level Agreement (SLA) will require a Root Cause Analysis to be performed and reported to the State's CCB
- **Availability Management**
    - High Availability and Enterprise Business Continuity and Disaster Recovery Plans (eBC/DR) will be tested and certified annually
    - eBC/DR plans will align with agreed upon Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO)

In alignment with TOGAF, the Integrator will align their solution with the State's Data, Application, and Infrastructure Architectural Domains. All artifacts will be maintained and updated as required to reflect changes to both business strategy and IT technologies.

Software

The eight components include the following:

1. **Identity Access Management/Single Sign On (IAM/SSO) -** All users, both internal and external, are validated through a common security portal using Security Assertion Markup Language (SAML) for authorization and authentication. Users maintain a single account for use across all consuming systems. The use of JSON Web Tokens (JWT) has also been approved.
2. **API Gateway (APIGW)** – Applications communicate through the APIGW to access other enterprise components and to integrate via web services (SOAP or RESTful) to systems both inside and outside of the State's network.
3. **Enterprise Service Bus (ESB)** – The ESB provides API connections to legacy applications and mainframe systems in addition to providing support for process queues. Access to the ESB is done via web services (SOAP or RESTful) or through message queues.
4. **Master Data Management (MDM) -** Stores common, shareable, reusable records, such as for an "entity" or a "person", to improve data integrity within and across applications statewide. Use of the MDM is highly encouraged by the State's Enterprise Data Management group to develop Statewide master person/entity relationships across the enterprise.
5. **Data Warehousing (DWH)** – Statewide data storage system that allows for cross application or even statewide reporting of information.
6. **Electronic Document Storage (EDMS) -** Document storage system that allows flexible and scalable storage of a variety of file types.

7. **Consumer Communications (CC) -** Allows for the production and distribution of internal and external communications via print, email, and SMS. The CC component fully integrates into the State's Enterprise Print Center for print and mail fulfillment.
8. **Business Rules Engine (BRE) -** Creates and maintains the rules that underlie the decision logic within an application.

Support Tiers

These components are separated into two support tiers. Contractors are required to utilize Tier 1 components for any system integration. Use of Tier 2 components is not mandatory but is highly encouraged where appropriate. The proposer should describe which Tier 2 components they intend to utilize and how they will be utilized.

Tier 1:

- Identity Access Management/Single Sign On
- API Gateway
- Enterprise Service Bus

Tier 2:

- Master Data Management
- Data Warehousing
- Electronic Document Storage
- Consumer Communications
- Business Rules Engine

In addition to these components, the EA system uses many software systems for reporting, monitoring, file transfers, workload scheduling, work management, application lifecycle management, and other ancillary functions.

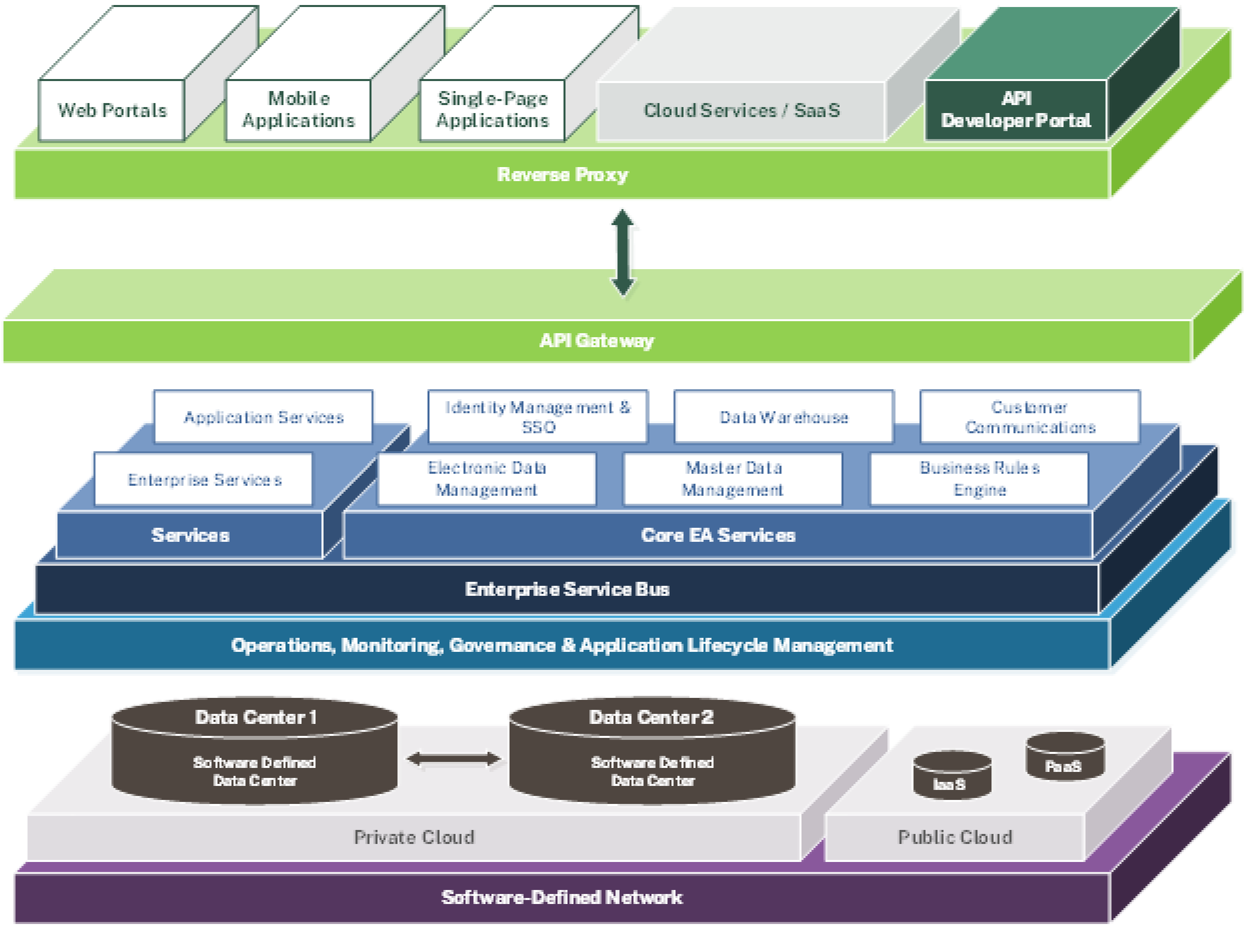

Figure 1 - EA Conceptual Model

Environments

The EA system provides three environments into which consuming systems to integrate. These environments are separated according to the data classification of any data processed by consuming systems, according to the data classifications rules in the OTS Information Security Policy. The three environments are:

1. **Production (PROD)** – Contains all production systems. The use case for this environment is for any production system. This environment is highly available, in an active/active configuration.

2. **Non-Production/Restricted (NPR)** – Contains non-production systems which consume or process restricted information. Use cases for this environment include User Acceptance Testing (UAT), Staging, and Conversion.

3. **Non-Production/Non-Restricted (NPNR)** – Contains non-production systems which consume or process non-restricted information. Use cases for this environment include Development,

System Integration Test (SIT), and Training. This environment is highly available, in an active/active configuration.

Additionally, the EA system has a single **Development (DEV)** environment which is not exposed for consuming system use. The Development environment is used for testing EA platform upgrades, hardware and software updates, and other system changes.

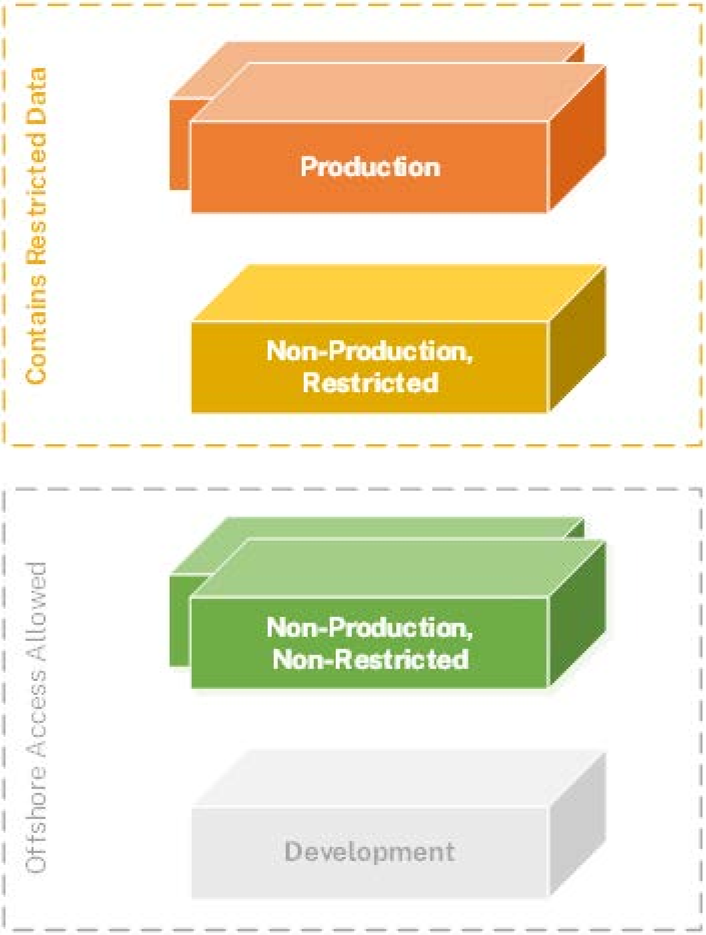

Figure 2 - Environment Design

Technology Stack

Version numbers are shown, where appropriate, and are subject to change

Infrastructure

Item	Vendor	Description	Version

Nutanix	Nutanix/Dell	Hyper-converged computing with compute, storage and virtualization consolidated into a single appliance	
VxRail	Dell	Hyper-converged computing with compute, storage and virtualization consolidated into a single appliance	
ESXi	VMware		
vCenter	VMware		
NSX	VMware		
SRM	VMware		
Windows Server	Microsoft	Standard OS for Windows	2012 R2
RedHat Enterprise Linux	RedHat	Standard OS for Linux	
MS SQL Server 2014	Microsoft	Enterprise Database/Storage Engine	Enterprise

Core Components

Item	Vendor	Description	Version
Decision Center, Decision Server	IBM	Business Rules Engine (BRE)	v8.x
Exstream	Opentext	Client Communications, Correspondence Generation (CC)	v9.x
Pentaho	Hitachi Data Systems	Data warehouse and Analytics (DWH)	v5.x
Case Foundation, Content Manager, Enterprise Records Foundation	IBM	Electronic Document Management (EDMS)	v5.x
webMethods	Software AG	Enterprise Service Bus (ESB)	v9.x
API Gateway	Broadcom	Enterprise API Gateway	
Identity Manager for Consumers and Business Users, Identity Suite, Single Sign On	Broadcom	Security integration product; includes access management, directory services integration capability, and identity management (IAM/SSO)	v12.x
InfoSphere	IBM	Master Data Management suite (MDM)	

Performance, Monitoring, & Lifecycle Management

Item	Vendor	Description	Version
Bamboo	Atlassian	Continuous Integration, Deployment, and Delivery	
GitHub Enterprise	GitHub	Source Code Repository	2.7
IBM Workload Scheduler	IBM	Job Scheduling	
Jama	Jama Software	Requirements Tracking & Control	
JIRA	Atlassian	Issue & Project Tracking	7.0
McAfee Enterprise Security Manager	Intel	DevOps/Automation	
MoveIT	Ipswitch	Enterprise Managed File Transfer	
Nagios	Nagios	Infrastructure monitoring/alerting	XI
NewRelic APM	NewRelic	Application performance monitoring	
Puppet Enterprise	Puppet	DevOps/Automation	
Splunk	Splunk	Operational Intelligence	

Contractor Requirements for Integration

Proposers shall describe how their solution will integrate with the State’s Identity Access Management/Single Sign On system for both internal and external users. Integrating systems must use this system for all authentication and authorization functions.

Proposers shall describe how their solutions will utilize the State’s Enterprise Service Bus and API Gateway for all API or real time interfaces, or any interactions with other EA or State technology components. All integrating connections must be made using standard SOAP/REST APIs or connectors or message queues within the Electronic Service Bus or API Gateway. The use of JSON Web Tokens (JWT) may be approved by the State.

Contractors shall utilize the State’s MoveIT platform for all file transfers. The preferred connection method is FTPS (FTP over SSL) which requires a server-side CA certificate - no self-signed certificate will be allowed. 256-bit, FIPS 140-2 validated AES encryption is used to protect any transmitted files from unauthorized use, theft, hacking and/or viewing while stored on State resources. PGP/GPG file type encryption is also required with an exchange of public keys.

Proposers shall describe how each Tier 2 component will be leveraged in their solution. If proposing an alternative to one of the Tier 2 components, proposers must describe their alternative solution in detail and explain why the approach is more beneficial to the State. This explanation must include financial and project impacts, preferably in the form of Return on Investment (ROI), and including information regarding any value added in respect to project implementation schedule, ease of implementation, and technology alignment.

If the proposer’s solution will not use a Tier 2 component, the Proposer must explain in detail why this approach is necessary and beneficial to the State.

Example Service Level Agreements (SLA)

Technical performance measures for system uptime and system response time shall be evaluated for any interface or portal established by the Contractor and for use by the State, including utilization by state employee, member or provider, State system, or State designee's system(s).   The State will measure performance with Service Level Agreements (SLAs) and where necessary penalize the Contractor with Liquidated Damages based on their performance. The State reserves the right to add new Service Level Agreements.

Service Area/Activity	Service Level Agreement	Liquidated Damage
System Performance Measures / System Uptime	Users shall be able to access the SYSTEM twenty-four (24) hours a day, seven (7) days a week, at a monthly uptime of 99.5%, with the exception of planned downtime due to system upgrades or routine maintenance. All planned downtime shall be communicated and agreed to by the State. Measures to be calculated based upon 24 hour periods, to the extent it is requested and mutually agreed upon in writing.	Two thousand dollars ($2,000) per business day, per instance of non-compliance until compliance is achieved and acknowledged by the State.
System Performance Measures / System Response Time	The System shall have an average response time of two (2) seconds. The average is calculated using the thirty (30) most current, contiguous business days. Transaction time measured using the standard Time to First Byte (TTFB) metric.	Two thousand dollars ($2,000) per business day, per instance of non-compliance until compliance is achieved and acknowledged by the State.