Enterprise Architecture and System Development Requirements

Louisiana Office of Technology Services

Enterprise Architecture 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 Management (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 (including checks), email, and SMS. The CC component fully integrates into the State's Enterprise Print Center for print and mail fulfillment. The CC component provides a full templating engine for document generation.
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:

Tier 1

Contractors are required to utilize Tier 1 components for any and all system integrations where the component functionality is required. Integrating systems may not provide overlapping functionality with Tier 1 components. Exceptions to these integrations may be allowed with State approval. Tier 1 components are:

- Identity Access Management/Single Sign On
- API Gateway
- Enterprise Service Bus
- Consumer Communications
- Electronic Document Management
- Master Data Management

Tier 2

Use of Tier 2 components is not mandatory but is highly encouraged where appropriate. Specific integrations will be approved by the State. Tier 2 components are:

- Data Warehousing
- 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.

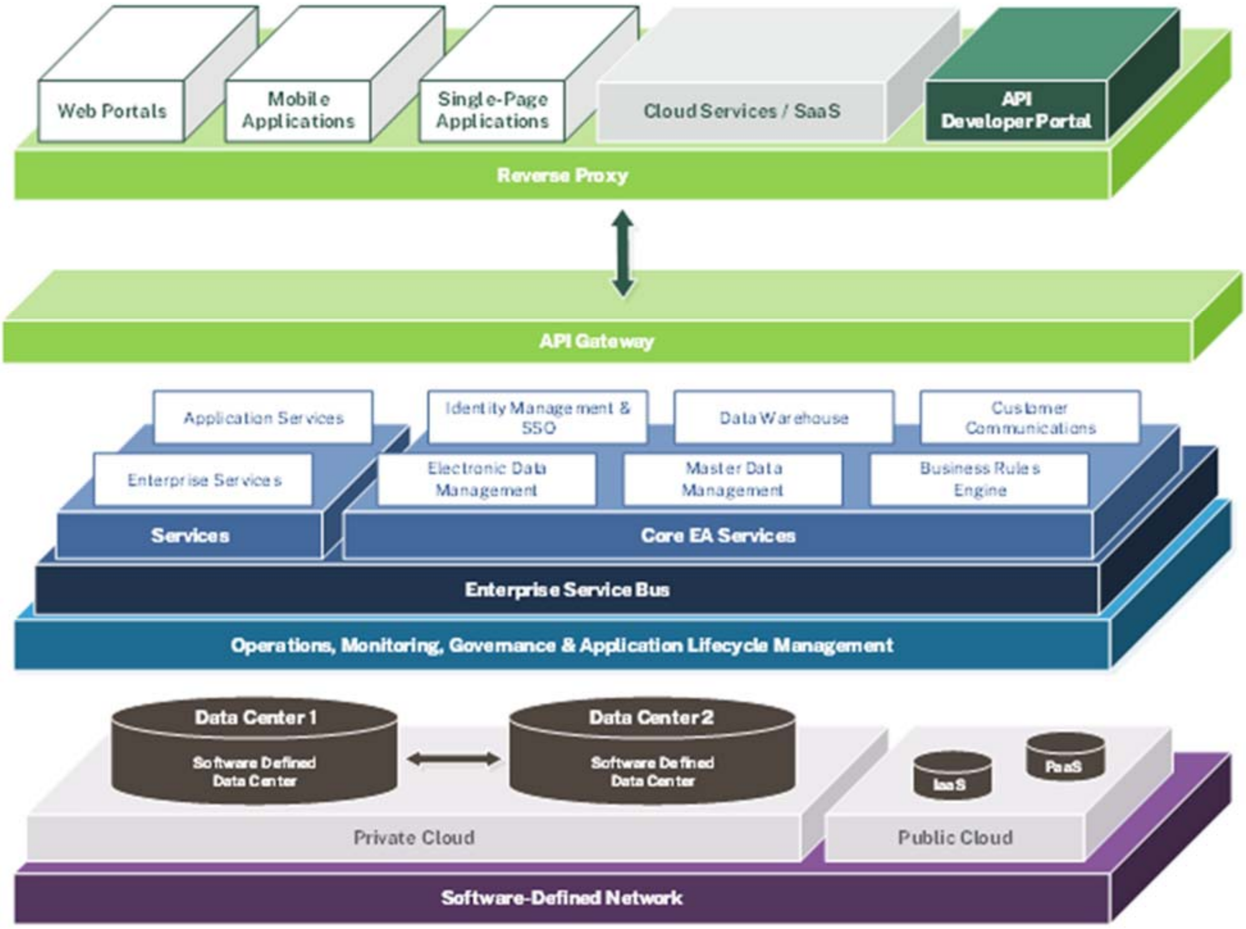

Figure 1 - EA Conceptual Model

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.

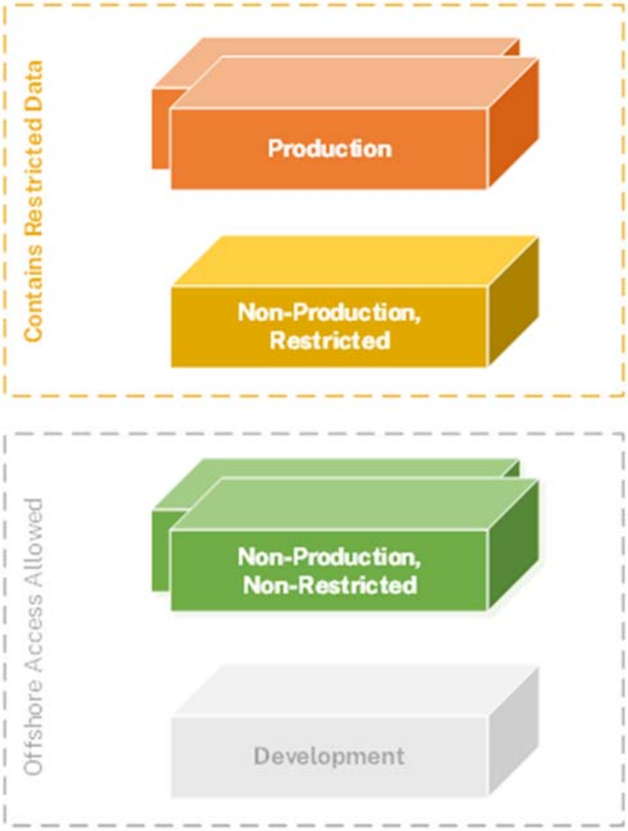

Figure 2 - Environment Design

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	

Item	Vendor	Description	Version
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 Cloud	GitHub	Source Code Repository, Continuous Integration, Deployment and Delivery, Package Management	
GitHub Enterprise	GitHub	Source Code Repository	3.1
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	
NewRelic Infrastructure	NewRelic	Infrastructure Monitoring	
NewRelic Browser	NewRelic	Browser Analytics	
Octopus Deploy	Octopus	Continuous Deployment and Delivery	2020.3.2
Puppet Enterprise	Puppet	DevOps/Automation	
Splunk	Splunk	Operational Intelligence	
Veracode	Veracode	Static Code Analysis	

Contractor Requirements for Enterprise Architecture 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.

System Implementation Requirements

The following requirements apply to all systems implementations:

1. Contractor shall use the State’s JIRA system to keep track of all features, user stories, issues, bugs and other application development lifecycle items.
2. Contractor shall design the UI to work on all browsers installed on the standard State computer image (Edge, Chrome & Firefox).
3. Contractor shall incorporate and test accessibility throughout the design and development processes to remain compliant with Section 508 Amendment to the Rehabilitation Act of 1973.

The following requirements apply to any systems hosted within the State’s infrastructure:

1. Contractor shall use NewRelic APM for application performance monitoring.
2. Contractor shall use Nagios for infrastructure monitoring.
3. Contractor should use Splunk for analysis and insights of logging and monitoring data.

System Development Requirements

The following requirements apply to any custom developed systems and applications:

Source Code Requirements

1. Contractor shall manage all assets (e.g., source code, automated tests, user stories, configuration files, knowledge transfer material, etc.) using the State's GitHub environments.
2. Contractor shall follow industry standard branching strategies (e.g. GitFlow, GitHubFlow).
3. Contractor shall use industry standard package management solutions for dependency management (e.g. NuGet, NPM, Maven, Pip)
4. Contractor should adhere to Twelve-Factor Application design methodology - http://12factor.net/.
5. Contractor should design the application architecture to ensure a separation of concerns and a reasonable degree of modularity between systems.
6. Contractor should adhere to the Don't Repeat Yourself (DRY) principle to ensure that the codebase remains flexible.
7. Contractor should ensure that all code will be written to a language specific code-style guideline to maintain consistency throughout the codebase.
8. Contractor should use an automated tool to evaluate the codebase and ensure compliance with the code-style guidelines.
9. Contractor should ensure all code written by one developer is reviewed by at least one other developer before merging into the mainline codebase.

Automated Testing

1. Contractor shall create and execute automated unit testing.
2. Contractor shall create and execute automated system tests to verify all features of the software module and all user facing functionality.
3. Contractor shall provide a summary of automated tests and the coverage statistics.
4. Contractor shall make the bugs identified during testing available to view real-time and on a historical basis.
5. Contractor should execute tests automatically on code merge into version control.
6. Contractor should use an automated tool that measures the amount of the codebase that is covered by tests.
7. Contractor should create and execute automated integration testing with other Contractor developed modules.

Load and Performance Testing

1. Contractor shall create and execute load and performance tests at regular intervals, and at each release.
2. Contractor shall provide a summary of all load and performance test results.

Accessibility

1. Contractor should use an automated accessibility testing tool.

User Interface

1. Contractor shall design the User Interface (UI) to be mobile-first.
2. Contractor shall design the UI using responsive design.
3. Contractor should use the State design system, Pelican.

Logging and Monitoring

4. Contractor shall implement centralized and continuous monitoring.
5. Contractor shall implement full audit logging.

Security

1. Contractor shall adhere to the State's Information Security Policy (ISP).
2. Contractor shall use an automated black/white box security scanning tool (e.g., Veracode) to ensure a minimal baseline of security throughout the development lifecycle, and at each release.
3. Contractor shall provide the results of the security scans to the State.
4. Contractor shall adhere to the HTTPS-Only Standard as outlined in https://https.cio.gov/.
5. Contractor shall adhere to the NIST 800-53 specifications.

Build and Deployment

1. Contractor shall provide continuous integration of source code into the source code version control system.
2. Contractor should use the State's Bamboo system, a continuous source code build tool that enables continuous deployment of all applications into testing and staging environments.
3. Contractor shall include mock test data that should be publicly accessible for development by other system developers and contractors which shall not include personally identifiable information (PII).

4. Contractor shall use at least one of the following methods to deploy code changes to a higher order environment (e.g., Integration, Staging) accessible by the Contractor with the issuance of a single command:
    a. Containerization (e.g. Docker Engine, Rkt, and Warden)
    b. Configuration Management tools (e.g. Ansible, Puppet)
5. Contractor shall submit server images to the State using a Deployment/Release tool at the conclusion of each sprint and upon major releases.
6. Contractor shall deploy builds to the testing, staging and production environments that will be provided by the State.

Service Level Agreements (SLA)

Performance Requirements

Contractor performance will be measured based on the following requirements. Failure to meet these requirements may be considered a breach of Contract.

1. 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, but not limited to, 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.
2. All required reports will be submitted according to a written agreed upon schedule. Extensions may be granted in writing by the State.
3. Defects shall be corrected in production within thirty (30) days or less from date of report. Exceptions may be granted by the State in writing. No more than 10% of open defects shall exceed the 30-day corrective period, excluding those defects explicitly excluded by the State.
4. All scheduled maintenance tasks (upgrades, patching, installations, environment build outs) shall be planned and time estimated, including all tasks to be performed whether by state or contractor staff. Once a baseline has been agreed to by the state, it may change only with the written acceptance of the State. Actual execution time shall not exceed the estimated planned time by greater than 10%.
5. For any Service Level Agreement, the 3rd, and each subsequent, occurrence of an incident resulting from the same root cause or from a documented and un-remediated systemic issue is an automatic breach of Contract.

System Performance

Contractor must comply with the following provisions, unless otherwise directed by the State Project Director:

This Section sets forth:

- The general levels of response and availability associated with the System
- The responsibilities of Contractor and State
- Processes for Defects and change management

Definitions:

- "Business Hours" – Monday - Sunday, 6:00 AM - 8:00 PM

- “Incident” – An unscheduled event that leads to loss of, or disruption to, an organization's operations, services, or functions.
- “Minute” – Any contiguous sixty (60) seconds
- “Hour” – Any contiguous sixty (60) minutes.
- “Daily” or “Day” – Any contiguous twenty-four (24) hour period.
- “Weekly” – Any contiguous seven (7) day period.
- “Monthly” – Any contiguous thirty (30) day period.
- “Annual” or “Annually” or “Year” – Any contiguous three hundred sixty-five (365) day period.

Contractor will not be liable for any failure to meet a Service Level Agreement resulting from events, causes, or responsibilities that are outside of Contractor’s control, including, but not limited to the State or its personnel or third-party contractors’ failure to meet the State’s responsibilities under the Contract, any State managed network, hardware or software issues, or as a result of events of force majeure as described in the Contract.

All planned downtime shall be communicated and agreed to by the State. Downtime must not exceed eight (8) hours per scheduled event, unless agreed upon by the State.

SLA	Performance Expectation
System Accessibility	Users shall be able to access the components twenty-four (24) hours a day, seven (7) days a week, at a monthly uptime of 99.5%, except for planned downtime due to system upgrades or routine maintenance. Specifically during the hours between 6:00 am and 8:00 pm Monday through Friday, the monthly uptime shall be 99.99%, except for planned downtime due to system upgrades or routine maintenance.
System Capacity	In the event of an incident impacting performance, the System shall have the capacity to process at least 50% of the average number of service calls per hour except for planned downtime due to system upgrades or routine maintenance. The average number of service calls are calculated as the average number of service calls per hour occurring between 6:00 am and 8:00 pm Monday through Friday over the past thirty days or other mutually agreed upon window.
System Performance	The System shall have an average response time of two (2) seconds. The average number of service calls are calculated as the average number of service calls per hour occurring between 6:00 am and 8:00 pm Monday through Friday over the past thirty days or other mutually agreed upon window. Transaction time measured using the standard Time to First Byte (TTFB) metric.

SLA	Performance Expectation
System Performance Reporting	The Contractor shall publish monthly, quarterly, and annual agreed upon performance reports

Incident Management

The following table lists expected user support service levels to be performed to support the System. The State Service Desk will assign an initial priority for user-reported problems to ensure that the most serious problems are addressed first. Priorities are defined here and in the System Operations and Maintenance Plan. The Priority information is taken directly from the State Standards.

- **Critical Priority -** Multi-component or critical functionality outages. Disruption to agency/State business where there is no alternative or workaround. Security, significant impact to business operations and/or financial implications to an agency/State.
- **Major Priority -** Multi-component or critical functionality outages. Serious disruption to agency/State business where there is no alternative or workaround. Severe security, significant impact to business operations, and/or financial implications to an agency/State. The business determines that the incident does not require a 24x7 response.
- **High Priority -** Single component or single critical functionality outage. Moderate disruption to agency/State business where there is no alternative or workaround. Security and/or financial implications to an agency/State.
- **Medium Priority -** Partial or limited functionality causing an operational impact for an agency/State or delays agency/State business. Prevents use of a fully supported service by an agency/State or individual**.** Issue has a possible workaround.
- **Low Priority -** Affects a small number of users with limited to no business implications to agency/State. Problem concerning minor items.

The contractor shall prioritize and resolve all issues reported to the help desk in the agreed upon timeframes:

Priority	Performance Expectation
Critical Priority	Resolution or plan for resolution: Within one (1) hour of a critical priority production issue being successfully reported to Contractor, Contractor will initiate a conference call/meeting to determine a Rapid Action Plan (RAP). Problems outside of Contractor's control do not apply. 24x7 Response until Incident is downgraded. **Updates to Agency:** Every 1 hour or as Agency requests
Major Priority	Resolution or plan for resolution: Within one (1) hour of a major priority production issue being successfully reported to Contractor, Contractor will initiate a conference call/meeting to determine a Rapid Action Plan (RAP). Problems outside of Contractor's control do not apply. 7am – 7pm, Monday thru Friday response until Incident is downgraded. **Updates to Agency:** Every 4 hour or as Agency requests
High Priority	Resolution or plan for resolution: Within one (1) hour of a high priority production issue being successfully reported to Contractor, Contractor will initiate a conference call/meeting to determine a Rapid Action Plan (RAP). Problems outside of Contractor's control do not apply. **Updates to Agency:** As Agency requests.
Medium Priority	Resolution or plan for resolution: Plan for resolution will be defined within the next build meeting. Problems outside of Contractor's control do not apply **Updates to Agency:** As Agency requests.
Low Priority	Resolution or plan for resolution: Plan for resolution will be defined within the next build meeting. Problems outside of Contractor's control do not apply. **Updates to Agency:** As Agency requests

Defect Management

The following are Defect severity classifications that will be used to prioritize Contractor's response to such Defects. Contractor will work to respond to reported Defects. The Contractor and the State will establish in writing mutually agreed upon dates for correction of Defects.

- **Critical** - Multi-component or critical functionality outages. Disruption to agency/State business where there is no alternative or workaround. Security, significant impact to business operations and/or financial implications to an agency/State.
- **High** - Single component or single critical functionality outage. Moderate disruption to agency/State business where there is no alternative or workaround. Security and/or financial implications to an agency/State.
- **Medium** - Partial or limited functionality causing an operational impact for an agency/State or delays agency/State business. Prevents use of a fully supported service by an agency/State or individual. Issue has a possible workaround.
- **Low** - Affects a small number of users with limited to no business implications to agency/State. Problem concerning minor items.

Severity/Priority	Performance Expectation
Critical	Resolution or plan for resolution: Within twenty-four (24) hours of a mutually agreed upon critical production defect being successfully reported to Contractor, Contractor will initiate short term and/or long term activities to remediate the defect (unless otherwise expressly agreed to by State and Contractor).
High	Resolution or plan for resolution: Within two (2) business days of a mutually agreed upon high production defect being successfully reported to Contractor, Contractor will provide a plan for resolution (unless otherwise expressly agreed to by State and Contractor). Contractor will remediate the defect within two (2) weeks (unless otherwise expressly agreed to by State and Contractor).
Medium	Resolution or plan for resolution: Within five (5) business days of a mutually agreed upon medium production defect being successfully reported to Contractor, Contractor will provide a plan for resolution (unless otherwise expressly agreed to by State and Contractor). Contractor will remediate the defect within four (4) weeks (unless otherwise expressly agreed to by State and Contractor).
Low	Resolution or plan for resolution: Plan for resolution, if required, will be defined by State and Contractor.

For defects that require tenant user acceptance testing as mutually agreed to by State and Contractor, the ability of Contractor to meet the requirements above for Defects reported by the State is directly dependent upon State resource availability to test, authorize, and validate the modifications in the Production environment, and, in the event that a data-fix is required, the State’s validation of the test execution of the data fix as well as the execution of the necessary database scripts in the Production environment. Time required waiting for State resource responsible tasks will not be considered in the time calculations associated with this Service Level Agreement.

If Defects are not reproducible in non-production environments, the State will approve access and provide access to the production environment to specified Contractor staff to triage the Defects and help determine the cause of the Defects. Upon determination of the cause of the Defect, resolution will occur in accordance with the Contract.

Contractor will establish internal quality assurance processes to promote standard processes for software development, consistency with approved requirements, effective unit testing and system testing, and accurate documentation.