

# Supplement 1:

Enterprise Business Intelligence  
Operations & Run Services and BI Project  
Services

## Table of Contents

<b>1.0</b>	<b>Enterprise Business Intelligence Operations and Project Services .....</b>	<b>3</b>
1.1.	Background and Overview.....	3
1.2.	In-Scope Enterprise BI / Data Warehouse Technical Environment Details .....	4
1.3.	Current Data Marts and Reporting Sources .....	5
<b>2.0</b>	<b>BI / Data Warehouse Operational Run and Maintenance Services .....</b>	<b>6</b>
2.1.	General Operating Requirements.....	6
2.2.	Information Technology Infrastructure Library (ITIL) Operations and Maintenance Services .....	6
2.3.	General Operational Process and Procedure Requirements .....	8
2.4.	Operational Run Services Requirements .....	9
2.5.	Sizing Considerations .....	9
2.5.1.	Business Intelligence CRM Ticket Statistics for Most Recent 12 Month Period.....	10
2.6.	Document Convention: Deliverable Identification .....	10
2.7.	General Scope: Run (Operate and Maintain) Services Responsibilities .....	11
2.8.	Support and Maintenance of the State's Enterprise BI / Data Warehouse Platform .....	11
2.9.	Run (Operate and Maintain) Responsibility Matrix .....	12
2.10.	Production/Version Control and Release Management .....	13
2.11.	Break/Fix Support.....	14
2.12.	Major/Minor Upgrades (Ongoing).....	14
2.13.	System/Environment Administration Support.....	16
2.14.	Program Management & Master Release Calendar .....	16
2.15.	Minor Change Services and Continuous Improvement.....	16
2.16.	Maintaining Solution and Operations Documentation .....	17
2.17.	BI / Data Warehouse Technology and Process Optimization Plan .....	17
2.18.	Transition Activities and Commencement of Billing .....	18
2.19.	Additional Services.....	19
<b>3.0</b>	<b>Ongoing Development and Evolution of the State's Enterprise BI / Data Warehouse Platform .....</b>	<b>20</b>
3.1.	Future Project Services Objectives.....	20
3.2.	Future BI / Data Warehouse Projects and Deployments: Contractor Support Requirements .....	20
3.3.	Identification of Future Work.....	21
3.4.	Development Life Cycle Proposals associated with Development and Enhancement Projects.....	21
3.5.	Future Project Services Pricing Response and Rate Card.....	21
3.6.	Submission and Acceptance of the Proposed Contractor Offer and Statement of Work associated with a Future Project .....	22
3.7.	Additional Work Requirements and Conditions .....	22
3.8.	Currently Identified Work and Enhancement Requirements.....	22
3.9.	Agency Adoption of the OIT BI / Data Warehouse Platform.....	23
<b>4.0</b>	<b>Knowledge Transfer and Educational Services .....</b>	<b>24</b>
4.1.	Overview .....	24
4.2.	Periodic/Ongoing Knowledge Transfer and Training .....	24
4.3.	Change Management/Communications and User Training.....	24
4.4.	Contract Conclusion Knowledge Transfer and Training .....	25
4.5.	Cooperation with State or Successor Contractor.....	25
<b>5.0</b>	<b>Project Requirements: Applies to All Project Implementation Based Work Contained in this Supplement .....</b>	<b>26</b>
5.1.	Project Management and Coordination Services .....	26
5.2.	Create and Maintain Project Plan .....	26
5.3.	Meeting Attendance and Reporting Requirements.....	27
5.4.	Utilize OIT's Document Sharing/Collaboration Capability.....	27
5.5.	System and Acceptance Testing Requirements.....	27
5.6.	Support the State's Performance of User Acceptance Test (UAT).....	28
5.7.	Pre-Production / Production Deployment Phase .....	28
5.8.	System Changes as a Result of Contractor Projects.....	29
5.9.	Project Completion Activities and Final Documentation Handoff.....	30
<b>6.0</b>	<b>Required Contractor Roles, Minimum Standards .....</b>	<b>31</b>
6.1.	Operational Run Roles and Staffing .....	31
6.2.	BI Project Roles and Capabilities .....	32
6.3.	Staffing and Time Commitment (Operational Run and Project Services).....	33
<b>7.0</b>	<b>Assumptions, Staffing and Support Requirements, Commercial Materials and Other Matters.....</b>	<b>35</b>
7.1.	Support Requirements .....	35
7.2.	Pre-Existing Materials .....	35
7.3.	Commercial Materials .....	35

7.4.	Personnel Considerations.....	36
<b>8.0</b>	<b>Service Level Requirements: State BI / Data Warehouse Projects .....</b>	<b>38</b>
8.1.	Service Level Specific Performance Credits.....	39
8.2.	Overall Contract Performance .....	41
8.3.	Monthly Service Level Report.....	42
8.4.	Service Level Commitments – Project Implementation Services .....	42
8.5.	Service Level Specifications .....	43
8.5.1.	Defect Resolution – Mean Time to Repair/Resolve (Severity 1 Items) .....	43
8.5.2.	Defect Resolution – Mean Time to Repair/Resolve (Severity 2 Items) .....	44
8.5.3.	Defect Resolution – Mean Time to Repair/Resolve (Severity 3 Items) .....	45
8.5.4.	Service Levels – Testing Performance.....	46
8.5.5.	Blocking Issues – Identification and Removal.....	47
8.5.6.	Regression Testing Performance – Issue Find/Fix Rate.....	48
8.5.7.	Code Coverage – Automated Test Beds.....	49
8.5.8.	Service Levels – Project Performance .....	50
8.5.9.	Issue Reporting .....	51
8.5.10.	Deliverable Acceptance.....	52
8.5.11.	Support of State User Acceptance Testing Activities .....	53
8.5.12.	Service Levels – Development Methodology Compliance .....	54
8.5.13.	Service Levels–Project Delivery–Build/Test Activities as a Percentage of Overall Activities.....	55
8.5.14.	Service Levels – Project Completion – Issues Detected and Resolved In Production.....	56
<b>9.0</b>	<b>Service Level Requirements: State BI / Data Warehouse Operations / Run .....</b>	<b>57</b>
9.1.	Service Level Specific Performance Credits.....	57
9.2.	Overall Contract Performance .....	59
9.3.	Monthly Service Level Report.....	60
9.4.	Failure to Report or Report Late after Mutually Agreed Dates .....	60
9.5.	BI Applications and Environments .....	60
9.6.	Period Service Level in Full Effect and In-Progress Service Levels.....	60
9.7.	Temporary Escalation of an SLO to an SLA.....	61
9.8.	State Provided Service Support Infrastructure Elements .....	61
9.9.	Managed Service: Service Level Commitments .....	62
9.9.1.	Incident Resolution – Mean Time to Repair (Severity 1 Outages) .....	63
9.9.2.	Incident Resolution – Mean Time to Repair (Severity 2 Outages) .....	64
9.9.3.	Incident Resolution – Mean Time to Repair (Severity 3 Outages) .....	65
9.9.4.	Service Availability – Application Availability.....	66
9.9.5.	System Performance and Responsiveness .....	67
9.9.6.	Incident Resolution - Issue Triage, Closure and Recidivist Rate .....	68
9.9.7.	User Interaction – Completion of Administrative, Root, DBA and Privileged User Adds/Deletes .....	69
9.9.8.	Security – Monitoring & Auditing – Security Breach Detection.....	70
9.9.9.	Job Schedule and Scheduled Reporting Performance .....	71
9.9.10.	Operational Process Control & Repeatability – Changes to Production Environments .....	72
9.9.11.	Service Quality – System Changes.....	73
9.9.12.	Service Timeliness – System Changes.....	74
9.9.13.	Data Accuracy .....	75

## 1.0 Enterprise Business Intelligence Operations and Project Services

### 1.1. Background and Overview

State of Ohio Business Intelligence (BI), a program within the Department of Administrative Services Office of Information Technology, provides enterprise decision support, analytics, data-warehousing, and information management solutions to State Agencies, Boards and Commissions, and institutions of higher education. The BI program currently serves over 130 state agencies and institutions of higher education and more than 3,000 direct users. State of Ohio Business Intelligence customers leverage standard reporting solutions, analytical tools, dashboards, and scorecards to make more informed decisions by getting the right information at the right time.

At present, State of Ohio Business Intelligence services are provided to customers using two technological platforms. The scope of this RFP is not the entire State of Ohio Business Intelligence Program but, rather, specific to one of the two technological platforms. Services in this scope will be provided as a component of and under the governance and strategic direction of the State of Ohio Business Intelligence Program. The scope of support and project work around this technological platform is detailed herein.

The purpose of Business Intelligence Program is to help the State realize the benefits of its business intelligence solution by:

- Assisting users in migrating from legacy reporting environments to the BI environment,
- Identifying and improving on data integration opportunities,
- Decommissioning silo systems and legacy data warehouses,
- Maturing the State's business intelligence practice, and
- Educating state Agencies on business intelligence capabilities and opportunities.
- Increase the State of Ohio's capabilities by deploying high impact and cost effective reporting, analysis and decision support systems and systems operations and management capabilities;
- Differentiate the State of Ohio wherever possible by providing unique offerings to State employees and State constituencies while providing best-in-class BI/Data Warehouse operational performance and capabilities;
- Support the migration of Agency and Enterprise reporting, analysis and decision support capabilities to a reliable, repeatable and world-class set of capabilities, standards and methods that are delivered in a cost effective and predictable manner;
- Operate and Maintain an Enterprise platform that is designed to drive overall consistency of Business Intelligence/Data Warehousing through the leverage of common systems platforms, consistent business processes and deploying/leveraging best practices wherever possible; and
- Operate the system utilizing modern capabilities, delivered under contemporary IT standards such as ITIL, software and testing Capabilities Maturity Model (CMM) and structured software development/implementation methodologies to ensure overall quality, operational agility, and alignment while supporting future requirements of the State of Ohio in a reliable and cost-effective manner.

The State of Ohio regularly reviews the applicability of Agency and State Operational systems associated with the operations, maintenance and support of its applications portfolio to seek opportunities to streamline the State's operations and business processes around core Business Intelligence and related Data Warehousing functions.

In conjunction with the State's review and development of its ongoing strategy, several opportunities have presented themselves that the State has prioritized as beneficial to the State enterprise. In general these areas

have been identified due to their ability to provide impactful and reliable Business Intelligence Services to all State Agencies.

The scope of this RFP is in three general areas:

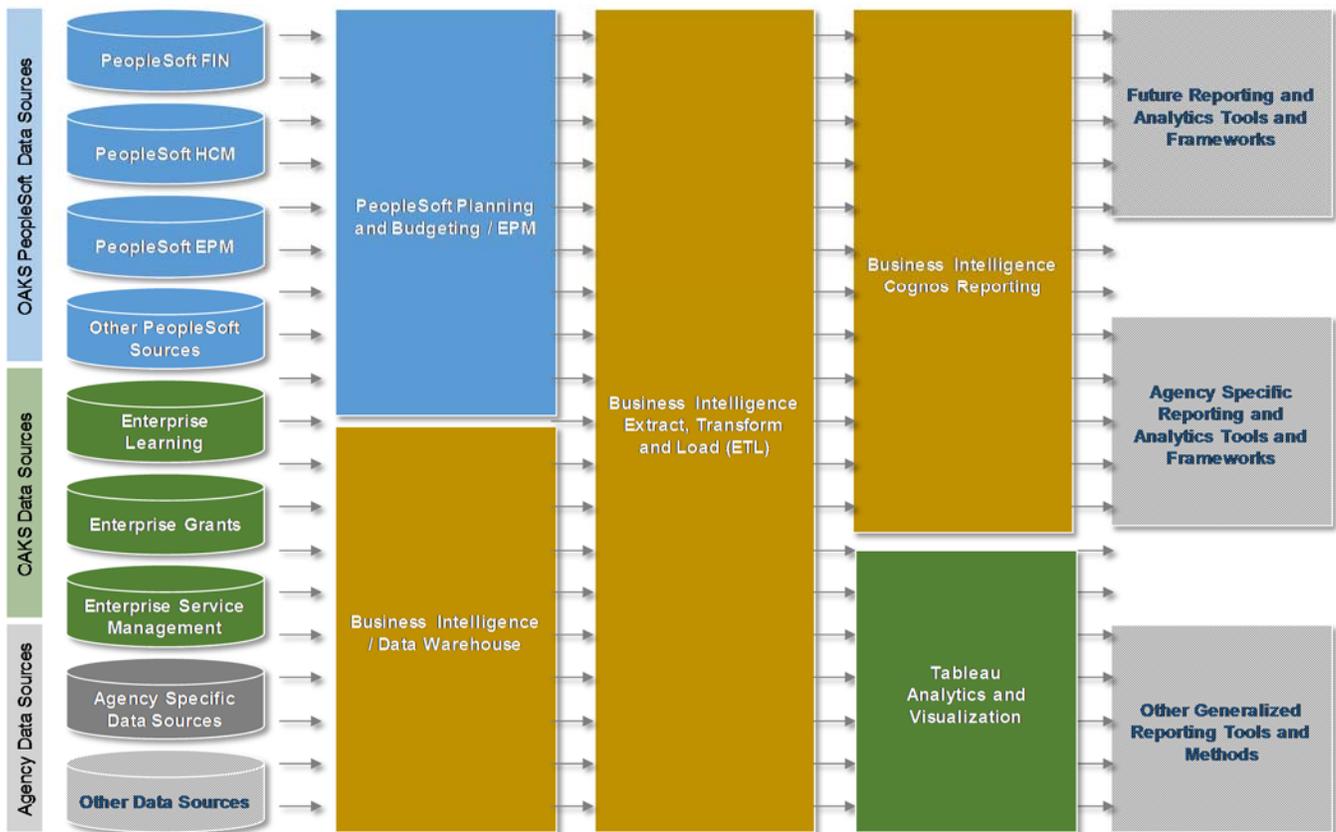
1. Operational Run and Maintenance Services for the State’s BI/Data Warehouse Environment;
2. Project Services to Enhance and Extend BI/Data Warehouse Capabilities within the State as projects; and
3. Agency Engagement/Adoption Services to assist Agencies in the best use of Business Intelligence and associated service offerings and (as required) incorporate and Agency Data in the Enterprise Data Warehouse as projects.

Requirements for each area are presented later in this Supplement.

**Offeror Note:** This RFP is not to replace any underlying technology, software or hardware components or to re-architect the Enterprise BI/Data Warehouse. The services requested in this RFP are limited to Operational Run Services and Projects associated with BI solution and expertise sharing and the coordination and harmonization of BI efforts across agencies, particularly those efforts that include the use of OAKS and other Enterprise Data stores and tools.

Conceptually, the enterprise BI/Data Warehouse platform subject to this procurement is as follows:

**Conceptual Organization of In-Scope Enterprise BI/Data Warehouse Elements**



**1.2. In-Scope Enterprise BI / Data Warehouse Technical Environment Details**

The Enterprise BI / Data Warehouse is comprised of the following technical and software elements:

Environments	Oracle DB Version	PeopleTools	Application
EPM 9.1	12.1.0.X.0 (12c)	8.53.XX	EPM 9.1 Bundle 4
Other Tools			
Cognos 10.2.1		IBM InfoSphere Data Stage 8.5	
Tableau 9.2.3		UC4, Tumbleweed and Agency Specific ETL Tools	

All data marts are currently EPM 9.1. This database size is approximately 6 Terabytes.

### 1.3. Current Data Marts and Reporting Sources

Data Marts	Source(s)	Target
Financials	PeopleSoft FIN 9.2	BI QA and Prod
Human Capital Management	PeopleSoft HCM 9.1	BI QA and Prod
Budget and Planning	EPM 9.1	BI QA and Prod
MBE/ EDGE	EPM 9.1	BI QA and Prod
ePerformance	PeopleSoft HCM 9.1	BI QA and Prod
ePAR	HCM 9.1 (Smart ERP)	BI QA and Prod
Enterprise Learning System	ELM 9.0	BI QA and Prod
State Payroll Projection System	EPM 9.1	BI QA and Prod
IT Spend	FIN 9.2	BI QA and Prod
SWCAP	FIN 9.2	BI QA and Prod
Value Management, Capital Improvements, Release & Permits, CAS, IT Investments, GSD Rent	Non-OAKS External Systems	BI QA and Prod

## 2.0 BI / Data Warehouse Operational Run and Maintenance Services

The Contractor will design and implement an Operational Run and Maintenance service that includes the following ITIL based high level processes for the BI / Data Warehouse platform:

- **Incident Management** – Manage service disruptions and restore normal operation quickly.
- **Problem Management** – Identify the underlying cause of recurring multiple incidents appearing related, (recurring related incidents).
- **Change Management** – Minimize the impact of service maintenance.
- **Configuration Management** – Define and maintain a configuration management database (CMDB).
- **Operational Reports** – Customized operational and maintenance reporting regarding platform performance, availability, uptime, users and other statistical information.

### 2.1. General Operating Requirements

The Contractor must design and deliver a set of operational run and maintenance services to provide the State:

- **High Degrees of Availability** – Agency customers and users will be able to use this service 24 hours a day, 7 days a week less any scheduled maintenance windows.
- **Seamless Continuity** – The Enterprise BI/Data Warehouse service must allow for seamless recovery from service disruptions.
- **Operational Efficiency** – This service must be delivered in a manner that requires fewer resources to meet the operational demands of the State Agency customer base.
- **Common Enterprise Operational Processes** – The BI / Data Warehouse is designed for all Agencies to utilize a common technology and process framework for complex and routine reporting, analytical, analysis and other data-driven decision making.
- **Global Administration** of the system, configuration, roles, permissions and the service licensing relationship with BI / Data Warehouse;
- **Maintenance, upgrades and releases** are which are scheduled and communicated no less frequently than monthly. Agency customer and OIT Service owner involvement are essential in providing User Acceptance Testing and reviews specific to release management and coordination.

### 2.2. Information Technology Infrastructure Library (ITIL) Operations and Maintenance Services

The State requires that the Contractor follow design and implementation principles which will continue the State use of Information Technology Infrastructure Library (ITIL®) compatibility. It is therefore required that the Contractor design and deliver services via a set of ITIL® v3 compatible concepts and techniques for managing the State's BI system.

Offerors are advised that the State OAKS team and related Business Unit functions have been operating under, and in many cases have been trained on ITIL principles and processes. Therefore Offerors are not to propose general ITIL training as part of their response.

The ITIL discipline has been implemented to be focused on providing the appropriate Services to support the following areas. The Contractor will propose, implement and utilize the following as part of its solution:

The **Service Desk** handles all in scope services incidents, problems and questions as well as providing an interface for other activities such as change requests, maintenance contracts, software licenses, Service Level Management, Configuration Management, Availability Management, Financial Management, Application Management, and IT Services Continuity Management for the Business Intelligence Platform inclusive of all tools, data and jobs.

**Incident Management** process and procedures are in place and continually refreshed in order to have the capability to restore a normal service operation as quickly as possible and to minimize the impact on business operations. An incident is considered to be 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. The objectives of the incident management process is to:

- Restore normal operations as quickly as possible with the least possible impact on either the business or the user, at a cost-effective price; and
- Maintain a comprehensive inventory of 'known problems' (without a known root cause) or 'known errors' (with a root cause) under the control of Problem Management and registered in an error database.

Processes and procedures include:

- Incident detection and recording;
- Classification and initial support;
- Investigation and diagnosis;
- Resolution and recovery;
- Incident closure; and
- Incident ownership, monitoring, tracking and communication.

**Problem Management** processes have been implemented to identify record, track, correct and manage problems impacting OIT service delivery. This area will be maintained to assist the State in recognizing recurring problems, addressing procedural incidents and containing or minimizing the impact of problems that occur.

The Contractor will support and follow established Problem Management processes to allow the State to find and resolve the root cause of incidents to minimize the adverse impact of IT infrastructure incidents and problems on the State and to prevent recurrence of incidents related to these errors.

The requirements of the Problem Management process are:

- Allow OIT to reduce the number and severity of incidents and problems on the business, and report it in documentation to be available for the OAKS support organization and end-users; and
- Allow OIT to provide a proactive process that identifies and resolves problems before incidents occur.

Implemented processes and procedures must include:

- Problem identification and recording;
- Problem classification;
- Problem investigation and diagnosis;

- Identification of the root cause of incidents;
- Trend analysis;
- Initiation of targeted support action;
- Providing information to the organization; and
- Iterative processing to diagnose known errors until they are eliminated by the successful implementation of a change under the control of the Change Management process.

**Change Management** processes and tools designed to minimize the impact of service maintenance to State operations and Agencies, inclusive of changes to production (code, process, configuration, reports and otherwise), controls with versioning, testing and verification and that change management and environment changes supported by BI processes and tools.

**Configuration Management** processes are implemented and followed for designing, planning and maintaining the physical and logical configuration of OIT services as well as 3rd Party integration and tool components and the way these resources are interrelated in the OIT environment. The Contractor shall employ ITIL compatible processes and tools that track all of the individual Configuration Items in the OIT service catalog for the supported infrastructure, software and service elements.

### 2.3. General Operational Process and Procedure Requirements

Contractor delivered processes and procedures must include:

- **Planning:** The Configuration Management capability shall be implemented to support planning of State service offerings for a rolling six months in detail, and a following twelve months in outline. It is reviewed with the State at least quarterly and include strategy, policy, scope, objectives, roles and responsibilities, the Configuration Management processes, activities and procedures, the database, relationships with other processes and 3rd Parties, as well as tools and other resource requirements.
- **Control:** This only accepts and records authorized and identifiable Configuration Items from receipt to implementation. The State provided infrastructure systems are under Change Management control.
- **Monitoring:** Accounting and reporting on all current and historical data concerned with each Contractor supported item throughout its life-cycle. It enables changes to items and tracking of their records through various statuses, e.g. ordered, received, under test, live, under repair, withdrawn or for disposal.
- **Verification:** Provide reviews and audits that verify the physical existence of items, and checks that they are correctly recorded in the Configuration Management database. It must also include the process of verifying Release Management and Change Management documentation before changes are made to the State live environment.
- **Service Catalog Management** – Automate requests for enhancements to the BI / Data Warehouse Environment from Agency customers to assist all parties in designing, operating and maintaining services across the Enterprise.
- **Knowledge Management** – Gather, store and share knowledge within OAKS OIT/ISD and Agency technical communities to drive awareness, standards and consistency of operations and maintenance functions.
- **Reports** – Customized reporting, dashboards for a variety of leadership, service owner and operational staff use that drive a consistent service and an understanding of all elements of the Service.

- **Other Future Capabilities** – Additional BI / Data Warehouse applications that the State may choose to implement in the future based on State priorities and preferences, which may be the subject of a change request issued by the State upon determination of need.

## 2.4. Operational Run Services Requirements

**Operational Services** processes will be implemented and followed that define the daily activities to deliver Enterprise BI /Data Warehouse services from the use of OIT infrastructure, applications, software and services in order to meet Service Level Agreements and established business targets for Agencies that use the environment. This collection of processes will be designed to adapt and respond to day to day fluctuations that occur in order to provide as much of the committed service as possible. This collection represents the day to day service operations within OAKS (as a service provider) and OIT/ISD (as an infrastructure provider).

This includes managing contact with the OAKS Service Organization, the OAKS Managed Service Provider (as applicable). Services include infrastructure, service and application management, event management, incident management, problem management and service execution.

**Offeror Note:** The State maintains a Governance and Oversight function designed to harmonize and ensure high quality operations and projects for the BI environment. This capability is known as the Business Intelligence Shared Council (BISC) and is comprised of OIT, Agency Finance and HR Professionals from across the State.

## 2.5. Sizing Considerations

In addition to the Operational Process Responsibilities and Service Level Agreements contained elsewhere in this Supplement, and in order to assist Offerors in sizing their proposals, teams and other factors as required to prepare a response.

The Contractor, as part of the work will maintain the business intelligence environment and support BI customers in the following areas. Provided frequency of support and involvement are representative based on historical use of the State and anticipated continued support requirements.

No.	Business Intelligence Support Summary Areas	Timing / Frequency
1	<b>Provide Training &amp; User Support</b>	
	<ul style="list-style-type: none"> <li>▪ Creating &amp; communicating monthly BI enhancement release notes and monthly training schedules, creating/administering project communication plans (as needed), scheduling and logistical support for training classes and conducting, instructor-led training classes.</li> <li>▪ This scope includes working with business users to offer customized training tailored to agency-specific needs, providing value management, creating/updating training materials (including new or tailored course content)</li> </ul>	Instructor- led Training --- Monthly 10-15 half and full day classes/sessions -currently 24 different courses.
2	<b>Tier 2 Customer Support</b>	
	<ul style="list-style-type: none"> <li>▪ Report assistance to agency builder (pointing to use of standard reports, tuning reports, running reports, report governance, adjusting filters and prompts, security)</li> <li>▪ Break fix existing reports (Errors and other)</li> <li>▪ Break fix variances between SRC-source and MDW due to any reason (Maintaining data accuracy with source)</li> <li>▪ Break fix due to sources out of BI Control</li> <li>▪ Moving reports due to upgrades</li> <li>▪ Other BI Support</li> </ul>	Monthly average of 40 Tickets (bulk of it is report assistance to agencies)
3	<b>Report Development</b>	

Nº.	Business Intelligence Support Summary Areas	Timing / Frequency
	<ul style="list-style-type: none"> <li>▪ Assisting with Business Analysis, requirements gathering and prioritization for new reports</li> <li>▪ Developing new Reports</li> <li>▪ Updating existing Reports</li> <li>▪ BISC (Business Intelligence Shared Council) approval of changes to Standard Reports</li> <li>▪ Providing Operations Management</li> </ul>	Monthly average 15 to 20 Tickets
<b>4</b>	<b>Enhancements/ Continuous Improvement</b>	
	<ul style="list-style-type: none"> <li>▪ Assisting with Business Analysis, requirements gathering and prioritization for enhancements</li> <li>▪ Assisting with enhancing existing BI capability ( reports /Model/ETLs)</li> <li>▪ Full cycle with new BI Capabilities - Plan, develop, manage, test, document and deliver</li> </ul>	Monthly 5 to 8 Enhancements
<b>5</b>	<b>ETL Development</b>	
	<ul style="list-style-type: none"> <li>▪ Support for Business Intelligence environment in regards to ETL (IBM InfoSphere DataStage) and Cognos</li> <li>▪ Develop new ETLs.</li> <li>▪ Update existing ETL's and models</li> <li>▪ Performance tuning</li> <li>▪ Migrations from Development to QA</li> </ul>	Monthly 5 to 10 Tickets and other maintenance as usual
<b>6</b>	<b>Framework Manager and Modeling</b>	
	<ul style="list-style-type: none"> <li>▪ Scope includes creating new Models</li> <li>▪ Maintain Models</li> <li>▪ Updates to existing Models</li> <li>▪ Sourcing new PeopleSoft Modules thus needing new marts</li> </ul>	Monthly 2 to 5 Tickets
<b>7</b>	<b>BISC- Business Intelligence Shared Council</b>	
	<ul style="list-style-type: none"> <li>▪ Scope includes facilitating BISC meetings</li> <li>▪ Working with the BI Service Owner in engaging the BISC and seeking approval for vendor created BISC content, major report changes/reviews and BISC messages</li> </ul>	Quarterly (but may vary per State needs)

### 2.5.1. Business Intelligence CRM Ticket Statistics for Most Recent 12 Month Period

To assist Offerors in understanding the complexity, size and operating considerations associated with the current BI environment, the following statistics are provided. Offerors are to note that these statistics are subject to change based on Agency use of the service and represent a point in time as opposed to a specific set of State requirements:

- Monthly average total is approximately 75. Lowest was 38 and Highest was 129.
- On average 50% of the tickets were closed within 24 hours' time period.
- 13 tickets were "High" Severity out of the 900+ tickets which were "Medium" Severity.
- Enhancements depend on the work type. It ranges from 3 days to 30 days typically.
- Enhancements spread is FIN 44%, HCM 37%, ePerformance 10%, other less than 10%
- 40+ enhancements were administered through the BISC review process.
- All Tickets closed after verbal or written confirmation

### 2.6. Document Convention: Deliverable Identification

All items in this Supplement that are marked with a red star (★) shall be considered formal deliverables and be subject to the State’s deliverable acceptance process described in Attachment 4, Part 5 of this RFP.

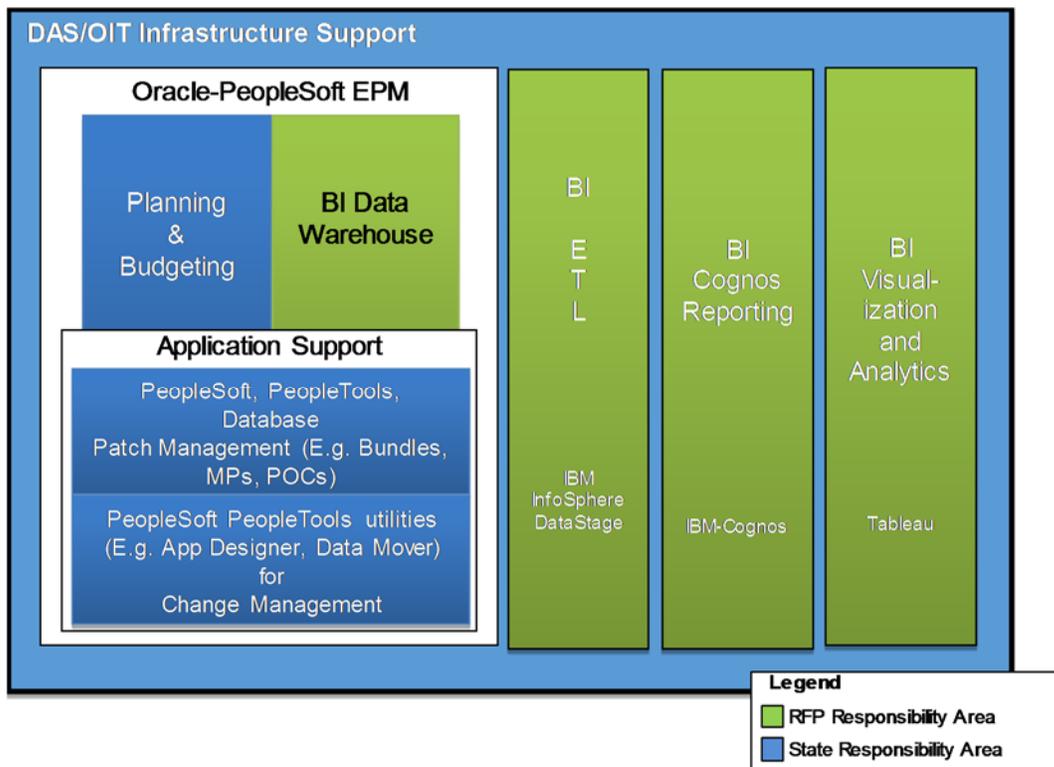
## 2.7. General Scope: Run (Operate and Maintain) Services Responsibilities

Based on activities and developments to-date, the following organizational chart has been created to outline the Contractor roles and functions as they would fit into the current team structure. To the extent that the Offeror believes an alternative team organization or structure would be beneficial to the State, the Offeror may present an alternative organizational chart and roles and responsibilities in the response to this section.

In general, the Contractor will maintain all extract/transform/load functions that feed the BI solution as well as data models, reporting and analytical functions within the State BI toolset (e.g. Cognos, Tableau). The State will operate, support and maintain the Planning and Budgeting (P&B) modules in EPM and common application support functions (e.g., standard Oracle provided elements including PeopleTools, databases, Oracle patches and updates, other OEM provided non infrastructure elements).

Conceptually these responsibilities are as follows:

**Conceptual Responsibilities: State & Contractor**



## 2.8. Support and Maintenance of the State’s Enterprise BI / Data Warehouse Platform

In high-level terms, Support and Maintenance of the State’s Enterprise BI system will include:

- BI / Data Warehouse application administration, reporting, and support;
- Supporting the State in re-testing or validating State specified PeopleSoft or Agency Source System RICEFW objects coincident with Major and minor BI / Data Warehouse system releases;

- Application Break/Fix responsibility and Minor Enhancements to State specified RICEFW objects;
- Migration to Production of applications once meeting the State’s acceptance criteria;
- Environment refresh services for non-Production and quasi-Production uses;
- System change management and Production version control; and
- Review of system usage, performance and reliability reports and collaboration with State Infrastructure Staff to drive system usability, reliability and performance.

## 2.9. Run (Operate and Maintain) Responsibility Matrix

The specific set of roles and responsibilities (RACI) pertaining to BI, Data Warehouse, Cognos, Tableau, EPM, and ETL scope between the State and the Contractor are as follows:

Nº.	Task/Function	State	Contractor
1	PeopleSoft EPM Application Maintenance (E.g. Bundle, Patch, MP, POC)	A, R	C, I
2	Maintain EPM Objects, Support & Enhance EPM pages not related to Planning and Budgets (P&B) e.g., SOPPS, MBE/EDGE	C,I	A,R
3	PeopleTools Maintenance (E.g. Patch, Upgrade, POC)	A, R	C, I
4	BI Functionality / Enhancement Releases	C,I	A, R
5	Planning & Budgets Functionality / Enhancement Releases	A, R	C, I
6	BI Customer Support	-	A, R
7	Planning & Budgets (P&B) Customer Support	A, R	C,I
8	BI Request Management	-	A, R
9	Planning & Budgets Request Management	A, R	-
10	BI Problem Management / Help Desk	-	A, R
11	Planning & Budgets Problem Management / Help Desk	A, R	-
12	Application Security Management for BI Warehouse components (Cognos, ETL)	-	A, R
13	Application Security Management for BI Warehouse Analytics/Visualization components (Tableau)	-	A, R
14	Application Security Management for PeopleSoft EPM (e.g. P&B)	A, R	I
15	Application Migration & Change Control for BI Warehouse (Cognos and Tableau)	I	A, R
16	Application Migration & Change Control for EPM Application (e.g. P&B)	A, R	I
17	Performance Tuning BI Warehouse (Cognos, ETL)	-	A, R
18	Performance Tuning BI Warehouse (Tableau)	-	A, R
19	Performance Tuning EPM Application & Oracle DB	A, R	C, I
20	PeopleSoft System Administration Tasks	A, R	I
21	Backup/Restore Management (Oracle DB, All Infrastructure Components)	A, R	I
22	Oracle Database Management	A, R	I
23	Oracle Data movement Activities (QA DB refresh, DB table backup)	A, R	I
24	Batch Scheduling and support for BI Warehouse	I	A, R
25	Batch Scheduling and support for Planning and Budgeting	A, R	-
26	Event Detection and Notification (Application & Infrastructure), System Alerts & Monitoring	A, R	I
27	Cognos, Tableau, ETL Application Maintenance (E.g. Upgrade, Update, Patch)	C, I	A, R
28	Cognos, Tableau, ETL Problem and Incident Management	C, I	A, R
29	System Administration Tasks (Cognos, Tableau, ETL)	C, I	A, R
30	Framework Manager/Modeling in Cognos	C, I	A, R
31	BI Training	C, I	A, R
32	BISC Logistics and facilitation	C, I	A, R

**RACI Key:** A = Overall Accountable, R=Responsible (implies Executes if not otherwise stated), C=Consulted (Assist, support, participate in order to concur), I=Informed

The Contractor will maintain the State’s BI / Data Warehouse environment and support State customers, inclusive of but not limited to the following:

1. Environment maintenance and support for Business Intelligence environment in regards to PeopleSoft EPM ETL (IBM InfoSphere DataStage), Tableau, and Cognos

2. Business Analysis, requirements gathering and prioritization for enhancements and new reports
3. Provide Operations Management
4. Manage and enhance data models and data marts
5. Develop Reports and ETLs
6. Provide Training, Organizational Change Management and User Support
7. This scope includes working with business users to offer customized training tailored to agency- specific needs, providing value management, creating/updating training materials (including tailored course content), creating & communicating monthly BI enhancement release notes and monthly training schedules, creating/administering project communication plans (as needed), scheduling and logistical support for training classes and conducting, instructor-led training classes.

## 2.10. Production/Version Control and Release Management

The Contractor will be responsible for working with the State and executing the production deployment and roll-out of any Release Package to the State's BI / Data Warehouse Environment.

Production deployment includes software deployment to the production instance of BI / Data Warehouse and (if applicable) interfaces to production tools and systems that orchestrate, manage, report or control those devices and services managed by the Service, identification of interfaces and any required conversions/migrations, installation of server software, and any required testing to achieve the proper roll-out of the Release Package software.

- ★ Contractor will establish and comply with the State required implementation and deployment procedures. This may include laboratory testing, migration procedures, the use of any pre-production or pseudo-production environment prior to production migration. Contractor will submit to the State, for the State's approval, a written deployment plan describing Contractor's plan to manage each such implementation. The tasks and activities to be performed by Contractor as part of the Deployment Services also include the following:
  - Establish procedures and automated software versioning mechanism(s) to ensure that the entire contents of a release, following State acceptance or authorization to implement to a production environment, are complete and maintain all elements that comprise the defined Release Package and the then current production version of the software prior to deployment of the Release Package to same;
  - Develop, prepare and test emergency back out or roll back procedures to return the production system to its pre-deployment State as it pertains to correcting an errant, erroneous or defective deployment of a Release Package to the production environment inclusive of all code, data, middleware, infrastructure, tables and parameters;
  - If, in the mutual opinion of the State and Contractor, the deployment of a Release package to the production environment is errant, erroneous or otherwise defective, implement back-out or rollback procedures in their entirety upon the written authorization or direction of the State.
  - If required, convert electronic data into a format to be used by the new solution using a data conversion program;
  - Conduct production pilot(s) (including "day in the life" simulations) and fine tune solution as mutually agreed with the State as appropriate;
  - Compile and maintain solution issue lists;
  - Conduct post Production Deployment quality and progress reviews with appropriate State personnel;

- Develop, and thereafter maintain and make available to the State, a knowledge base of documentation gathered throughout the Release Package’s life and allow for re-use of such documentation for future Projects; and
- Establish a performance baseline for the impacted business systems, and where appropriate document requirements for future enhancement of the business systems implemented as part of a future Project or Authorized Work.

## 2.11. Break/Fix Support

The Contractor will:

- Track, monitor and provide remediation for solution defects and incidents requiring system configuration or in-scope environment code or configuration changes;
- Identify and implement required system or configuration changes to address solution defects;
- Maintain solution documentation (technical specifications and testing documentation) as well as a compendium of common problems, root causes and remedy to aid in the identification and remediation of underlying system incidents;
- Test configuration changes to confirm resolution of defects;
- Support the State in performing applicable acceptance testing or review of any changes arising as a result of break/fix or patch/release Contractor responsibilities; and
- Ensure compliance with any State security or BI / Data Warehouse mandated patches or system levels to the extent and system enhancement turnaround time required given the nature of the security mandate and report to the State in writing any risks or issues that the Contractor becomes aware of in providing Service to the State. For example: patches designed to address immediate or active Security issues may be scheduled for a near-real-time release, where other less pressing releases may be implemented during a scheduled maintenance or outage period.

## 2.12. Major/Minor Upgrades (Ongoing)

Release upgrades for packaged software are initiated through periodic releases by BI / Data Warehouse as Major or Minor releases. Due to the packaged nature of these releases associated with the BI / Data Warehouse platform (i.e., unified patch streams that apply to the PeopleSoft, IBM, Cognos, and Tableau software, security and other elements), the State requires that the Contractor lead and coordinate efforts to analyze, install/apply, test/verify and utilize State specified RICEFW objects to these releases in the State’s environment. As the State is dependent on BI / Data Warehouse and is responsible for Enterprise reporting and analysis functions, this coordination and leadership must be well defined and executed so that the State can realize the benefits of a release while not introducing any service impacting or application related issues.

Further, the State understands the importance of BI / Data Warehouse major and minor upgrades to its overall capabilities in support of the State’s mission and in particular over the life a multi-year contract and is committed to maintaining the State’s BI / Data Warehouse system and related services at the most current proven release at all times, unless the State provides a written exception, in such a manner as to maintain ongoing compliance with BI / Data Warehouse requirements for maintenance of BI / Data Warehouse system and Contractor provided elements that comprise the BI / Data Warehouse system.

Contractors are to comply with the following:

- The State's requirement is to always operate on a set of Application and Technical Infrastructure components that are on the current BI / Data Warehouse release and support model and terms as utilized by the State in BI / Data Warehouse environments;
- As part of annual planning and coincident with monthly project review meetings, the Contractor is to inform State of any components that are moving beyond a current support model or would be rendered unusable as a result of an upcoming release and present a plan to implement the required updates in a controlled manner to the applicable State environment(s) to maintain compliance BI / Data Warehouse support models;
- Based on review of any upgrade or update plan (inclusive of all elements required to effectively manage, resource, test, validate and implement the change as outlined elsewhere in this statement of work, the State and the Contractor will schedule a mutually agreeable upgrade / update effort and authorize the Contractor to perform these upgrade services to maintain the required support model;
- Upgrade and update efforts must factor any regularly scheduled batch processing or system availability as well as any seasonal processing requirements and should be scheduled to maintain compliance with system availability in consideration of then prevailing development release or production schedule;
- The Contractor will be responsible for the design, development, and implementation of the Minor/Major enhancements in the State environments including requirements/design discussions, applicable conference room pilots, design review/signoff, document design specification, document and execute unit and integration/interface tests, support of the State in executing UAT;
- The Contractor must support the State in the planning and deployment of periodic releases of non-emergency patches and enhancements (e.g., test new functionality, regression test entire application, document release notes, coordinate with the State for end user change management/communication) as well as perform these responsibilities for all Contractor developed elements for the State;
- The Contractor must be capable of verifying and accepting enhancements not developed by the Contractor (e.g., review designs, execute tests, migration to production);
- All System Enhancements will be performed in accordance with the appropriate software development lifecycle procedures in this Supplement; and
- For all code based deliverables that are accepted by the State or otherwise placed in commercial use, the Contractor will provide an electronic copy of all source and executable code elements to the State as part of the deployment of the element's introduction to production or commercial use.

Notwithstanding Major and Minor Upgrade enhancement requirements as outlined above, the Contractor has an obligation to maintain all BI / Data Warehouse elements in keeping with a current support and in accordance with agreed procedures associated with the minimization of exposure to viruses, security holes or flaws, incompatibility issues, software patch currency, technical updates, corrections and other elements that directly influence the warrantee, support, performance and ongoing upgradeability of underlying software and State specified RICEFW objects of the BI / Data Warehouse system.

Upgrades and updates will be scheduled in such a manner as to:

- minimize disruption to State operations and use of the BI systems by Agencies;
- balance capital requirements with State priorities and availability of funding;
- balance risk to the State as to ensure that BI releases are scheduled as to not conflict with other efforts to deploy elements to production or as to interfere with production job schedules;
- utilize new releases of software (e.g., Cognos, PeopleSoft, Oracle and Tableau) when available from the OEM software providers; and

- balance Contractor staffing availability and synergies to provide a seamless and overall consistent upgrade approach.

**The Contractor will propose fixed pricing for performance of these upgrades in keeping with these timing considerations that are applicable to the overall term of the agreement.**

### 2.13. System/Environment Administration Support

The Contractor will:

- Perform BI / Data Warehouse technical activities including but not limited to: system code/object migrations, patch implementations, log administration, data copies and exports, interface and scheduled reporting/ETLs, and responsibility for incident resolution such that migrations into production will be executed at agreed periodic intervals and other production changes will be scheduled during the maintenance window.
- If required, support multiple release levels of System software/hardware elements for in-scope Services, provided that such support does not impair the Contractor's ability to meet Contractor development and project commitments until such time as all environments can be upgraded to the same version/release level.

### 2.14. Program Management & Master Release Calendar

The Contractor follow the State established Master Release Plan and support the State in the development, maintenance and publication on a monthly basis of a Master Release Calendar that includes a schedule (with dates) of:

- Major/Minor and Scheduled Releases, Upgrades, Updates and Enhancements;
- Implementation of Projects, Minor Enhancements or Discretionary Work;
- Scheduled Maintenance Windows and Planned Outages;
- Major and Minor Project Key Dates (i.e., Start, SDLC Gate Completion, Production Release, Completion) whether Contractor delivered or otherwise; and
- Other pertinent dates that require end-user notification or coordination.

### 2.15. Minor Change Services and Continuous Improvement

Based on the State's experience with the management and ongoing operations of the BI environments, the State is requiring the Contractor to provide the capability to address minor alterations or enhancements to Applications within the scope of the Services that arise as a result of legal, regulatory, mandates or changes to the State's business. Due to the nature of these requirements (e.g., minor display field changes, edits, reports, etc.), the State may require the Contractor to provide these services as needed.

- The Parties will agree to a resource plan to support discretionary services in order to maximize personnel continuity.
- The Contractor must include, in their proposed annual cost for discretionary/Continuous Improvement (CI) hours, an initial pool of eight thousand (8,000) annual hours to be used in conjunction with the Contractor's Rate Card, and represent an initial minimal monthly staffing level of four full-time equivalents. The hours will be pro-rated for the first Contract fiscal year commencing July 1<sup>st</sup>. Discretionary/CI hours will not be applicable for use for any other services contained within Section 2 of this Supplement. Should, for whatever reason hours not be utilized in a given fiscal year, those unused hours shall carry forward to the following fiscal year. Prior to final year of the contract, the State will establish a final pool of hours inclusive of any unused hours from the prior contract year.

- The Contractor and State will meet quarterly beginning 90 days following Contract execution to review this discretionary/CI hour pool and make adjustments at the sole discretion of the State.
- The Contractor will provide a schedule of discretionary/CI hours consumed (by activity, resource and Project) and a forecast of remaining hours and activities to the State on a monthly basis.
- For the avoidance of doubt unless otherwise specified, all services within Section 2 with the exception of Section 2.15 (this section) are to be provided as a fixed-fee, base service and not subject to cost variability.

Ad-Hoc Requests may be required under this discretionary/CI hour pool. The following provides an example of ad-hoc requests:

- Ad-hoc requests require no modification, configuration, or customization of the environments.
- Routine tracking procedures will provide visibility of all ad-hoc requests to the State Authorized service representative. The Contractor and the State will develop a prioritization approach for ad-hoc requests based upon business impact and document such process as mutually agreed.

## 2.16. Maintaining Solution and Operations Documentation

★ Contractor will:

- Document the solutions developed or modified by the Contractor in accordance with established methods, processes, and procedures such that, at a minimum the State or a competent 3<sup>rd</sup> Party vendor can subsequently provide a similar scope of Services;
- Develop and maintain, as agreed appropriate, the documentation on system environments. Where it is determined that documentation is inaccurate (for example, due to demonstrated errors or obsolescence), and such inaccuracy may negatively affect the Services, Contractor will correct such documentation as part of normal day-to-day operational support;
- Update programmer, End User and operational reference materials;
- Maintain all documentation on the State's SharePoint site and ensure that all documentation is current following any change to the BI service or BI / Data Warehouse as it relates to documentation and conduct an annual audit for State review of all documentation to ensure ongoing compliance with these requirements; and
- Contractors will comply with State IT Access policies for State systems, offerors are to note that this compliance may require the provision of certain Contractor personnel related identifying (but anonymous) information to establish Contractor personnel on State systems such as insignificant (last 4) digits of SSN or Driver's license information.

## 2.17. BI / Data Warehouse Technology and Process Optimization Plan

The Contractor will create and follow a technology and process optimization plan that is aligned with contemporary best practices and in keeping with the achievement of OIT's Service Level Agreements (SLAs) provided to Agencies. Based on Contractor best practices, and in keeping with the OIT's attainment of the defined SLAs, the Contractor must propose a specific approach that is achievable within BI / Data Warehouse or propose an alternate business practice with a detailed description and rationale that include:

- Refinement of existing service specific toolsets, environments and operational processes to ensure overall continuity and minimization of late-term disruptions or diminishment in services due to opportunities to optimize the BI / Data Warehouse platform and how it operates; and
- Phased replacement or enhancements to operational and technical processes over the term of the Contract to best leverage existing State investment in technology components, use of personnel (both State and

Contractor) while minimizing any disruptions in service associated with the implementation of the operational or technical processes.

In any case, Contractors are specifically required as part of the technology and service optimization plan to:

- Provide and implement a plan to include existing or future OIT technology services or elements (whether production or non-production); and
- Adjust processing, configuration, job schedules or operating processes/procedures to leverage the State’s investment in the BI / Data Warehouse infrastructure and software while minimizing manual labor, work/re-work cycles, non-productive endeavors or other elements that would allow the State to deploy, operate and manage OIT services in a more optimal fashion.

## 2.18. Transition Activities and Commencement of Billing

The Contractor shall **NOT** invoice the State for Operational Run Services until the following criterion are met:

- All Contractor personnel are staffed and present to perform services as required under this RFP;
- All transition and knowledge transfer activities from the Current BI Operations Vendor are completed and the Contractor is in control and responsible for the Operational Run Service;
- Contractor demonstrates proficiency in each of the following 3 areas (OAKS Operating Model, BI Environment/Tools, and BI Data Model) by having a composite score of 4 out of 5 as scored by the sole discretion of the State. This is shown in the table below:

Area	Description	Score (1-5)
<b>1</b>	<b>OAKS Operating Model</b>	<b>Mean (1a:1e)</b>
1a	Managed Services and State of Ohio Computing Center Relationship	(1-5)
1b	OAKS ITIL Processes	(1-5)
1c	OAKS Run Book	(1-5)
1d	OAKS Business and Commerce	(1-5)
1e	BI Governance Process	(1-5)
<b>2</b>	<b>BI Environment/Tools</b>	<b>Mean (2a:2g)</b>
2a	Infrastructure	(1-5)
2b	Databases	(1-5)
2c	Operating Systems	(1-5)
2d	PeopleSoft Applications	(1-5)
2e	Cognos	(1-5)
2f	Tableau	(1-5)
2g	DataStage	(1-5)

<b>3</b>	<b>BI Data Model</b>	<b>Mean (3a:3k)</b>
3a	Financials	(1-5)
3b	Human Capital Management	(1-5)
3c	Budget and Planning	(1-5)
3d	MBE/ EDGE	(1-5)
3e	ePerformance	(1-5)
3f	ePAR	(1-5)
3g	Enterprise Learning System	(1-5)
3h	State Payroll Projection System	(1-5)
3i	IT Spend	(1-5)
3j	SWCAP	(1-5)
3k	Value Management, Capital Improvements, Release & Permits, CAS, IT Investments, GSD Rent	(1-5)

Note that billing may start the month that transition completes. The first month's invoice will be prorated as necessary to reflect the number of days the vendor is performing the BI Run Managed Services after transition. The Contractor will not be reimbursed for activities during the transition period, all such costs must be included in the Contractors Operations Run costs during the base contract period.

## 2.19. Additional Services

The following additional services are to be provided by the contractor:

- To the extent an incident is due to errors or defects within an in-scope environment, supported service or element licensed by a 3<sup>rd</sup> Party to the State that interfaces with or provides data to BI, the Contractor will assist the State by referring such incident to the appropriate 3<sup>rd</sup> Party entity for resolution and coordinating with the 3<sup>rd</sup> Party contractor or software provider as appropriate to help minimize the State role in problem management.
- If directed by the State under an approved I/D/A, address functionality gaps or data elements not present in the data warehouse by adding new tables, fields and data marts to the BI Service Offering.
- If directed by the State under an approved I/D/A, promote adoption of the BI Solution as an integrated component of OAKS and OIT enterprise services through outreach and customer engagement, enhancements, new functionality and integrations with other systems.
- Assist in the detection of, and if directed by the State under an approved I/D/A, resolve any upstream source system data, data feeds, interfaces, integrations, Extract Transform Load (ETL) routines or provide PeopleSoft specific expertise to address deficiencies in the State's PeopleSoft environment as to remediate issues within such environments or (onwards) to BI / Data Warehouse data, analysis/reporting structures or reports as required within Enterprise Reporting tools (currently Cognos and Tableau) Agency reporting tools as required.
- Implementing measures to help avoid unnecessary recurrence of incidents impacting the BI / Data Warehouse platform, by performing root cause analysis and event correlation.

### 3.0 Ongoing Development and Evolution of the State's Enterprise BI / Data Warehouse Platform

The State may from time to time request proposals in the form of Statements of Work (SOW) e.g., Change Request/Amendments or Interval Deliverable Agreements (IDAs) under the contract arising from this RFP for the design, development, testing and deployment of new applications or significant application enhancements ("Application Development Projects"). Upon completion of a Project Services implementation, the completed application, once meeting the State's acceptance criteria, will, in most cases, be managed by the State on an ongoing basis as an Enterprise DAS/OIT service.

The State may also request hourly consultative expertise services pertaining to business, functional or technical expertise from the Contractor. When such services are provided by the Contractor that do not involve full lifecycle development or implementation responsibilities, the Project Requirements described in this Supplement under Section 6 may not apply (determined at the sole discretion of the State). The State acknowledges that it is responsible for the management of these types of projects and of the work being provided by any Contractor staff providing services under such an engagement.

#### 3.1. Future Project Services Objectives

The Future Project Services are defined to achieve the following:

- Standardize the Delivery Model for new application development using the Enterprise BI / Data Warehouse Platform;
- Facilitate smooth, well-defined transitions of new Projects to steady-state/production (Run Services) support;
- Utilize the Contractor's rate card to better control overall development costs across the State;
- Improve delivery through clearly defined development standards, conventions and guiding principles;
- Implement a standards based governance structure to drive process improvements and consistency across the State;
- Speed up the development lifecycle by reducing the procurement timeline; and
- Identify, design and develop Agency specific Security and Data privacy requirements that follow State standards included in Supplement 2 as well as any Agency specific requirements based on Agency use of the BI / Data Warehouse platform.

#### 3.2. Future BI / Data Warehouse Projects and Deployments: Contractor Support Requirements

The State has invested in the creation and ongoing operation of the BI / Data Warehouse platform. As a result of ongoing BI / Data Warehouse releases, stabilization and extension into new lines of business and services as well as current IT Optimization efforts underway State-wide, the State has identified several opportunities for Agencies leverage BI / Data Warehouse based platforms in support of the State's overall, and Agency-specific missions.

The Contractor will support DAS/OIT in:

- The development and refinement of ongoing BI / Data Warehouse Business Roadmaps for State identified BI / Data Warehouse opportunities;

- Creation of business case, change programs for BI / Data Warehouse adoption/extension budgets, timelines and investment models that are pragmatic and grounded in the realities of budgets, implementation efforts and BI / Data Warehouse capabilities;
- Development and delivery of exploratory workshops with new Agency customer groups from the above;
- Leading of “change agent” type communications designed to encourage Agency and Statewide adoption of BI service offerings; and
- Support DAS/OIT management in bridging: business, functional and technical and organizational changes to propose, design, implement and extend BI / Data Warehouse offerings Statewide.

### 3.3. Identification of Future Work

Contractor’s responsibilities with respect to identification of future work will include the following:

- Submit project or improvement ideas, and agree to a development roadmap to more optimally deploy, operate and maintain the Enterprise BI / Data Warehouse, State and Contractor extensions and enhancements and State processes.
- Collaborate with the State to identify and support Agency specific BI / Data Warehouse needs inclusive of Agency specific data, integration of Agency and BI/Data Warehouse Data or OAKS data as required.
- Streamlining or eliminating sub-optimal processes (technical, performance, organizational and work-effort) that surround the operation and maintenance of the BI / Data Warehouse, whether in the Contractor’s responsibility or those provided by the State for Contractor use or those that impact the timeliness, quality or cost of OIT services to Agency customers.
- Review of BI / Data Warehouse Service Level performance and discussion of increasing service delivery quality to OIT customers through improvement of visibility of operational performance, bottlenecks, I/P/C processes and SLA performance via adjustments or enhancements to State specified RICEFW (Reports, Interfaces, Configurations, Extensions, Forms and Workflow) objects.
- Upon the State’s request, develop a non-binding rough order of magnitude schedule and cost for consideration and following this consideration or upon direction of the State, develop a formal pricing and Statement of Work inclusive of delivery dates, requirements, scope, deliverables and other implementation specifics for the State’s authorization to proceed as defined within Section 5 of this Supplement pertaining to Interim Development Agreement(s) or I/D/A.

### 3.4. Development Life Cycle Proposals associated with Development and Enhancement Projects

The Contractor will provide a disciplined Systems Development Life Cycle (SDLC) methodology for use on Application Development Projects and will adhere to such methodology during the performance of Application Development Projects. The Contractor will adapt this methodology as required to meet the State’s needs. The Contractor will provide the State with a comprehensive description of the methodology, the formal training available if required, the development tools and templates used with the methodology, the project management tools to be used with the methodology, and the plan for implementing the methodology within the State environment. For large changes and releases the Production/Version Control and Release Management requirements in Section 2.10 above must be followed.

### 3.5. Future Project Services Pricing Response and Rate Card

Unless requested by the State in a deliverables based arrangement, Contractors must utilize the Rate Card, by project personnel role and experience level as well as Technical role and experience level that is binding over the Contract term. The Contractor may not propose rates in any Project SOW that differ from this rate card as allowed under any contract arising from this RFP.

### 3.6. Submission and Acceptance of the Proposed Contractor Offer and Statement of Work associated with a Future Project

At the State's request, the Contractor must provide an offer that addresses the State's SOW for an Application Development Project. The Contractor's offer must incorporate the SDLC described above (or as agreed to by the State) and as appropriate, be in accordance with all the requirements included in both the Mandatory Project Management and Execution sections of this Supplement. At a minimum, the Contractor's offer must include a list of activities to be executed and deliverables to be created, organized by SDLC Phase (e.g., design, build, test and implement).

The Contractor's offer must be priced based on either the Rate Card (for time based projects) or Fixed Price Deliverables/Milestones included in the Cost Summary for the completion of the deliverables required by the State's requirements and as contained in a mutually agreeable SOW.

The State will review the Contractor's offer and provide feedback as needed to the Contractor within thirty (30) days of receipt of the offer. Under no circumstances will work be started without State approval, and the State will have no financial obligation for services performed without State approval.

Upon State acceptance of a Contractor Proposal, all standards, conventions and general Project Management requirements contained in this Section 6 of this Supplement shall apply unless otherwise agreed to in writing by the State.

### 3.7. Additional Work Requirements and Conditions

The following identify additional work requirements and conditions for Project or staff augmentation services:

1. Contractor staff must submit time sheets for all time and materials work (for that work that is time and material based) to the State for review and approval on a monthly basis and a formal Deliverable or Milestone approval sheet for that Work that is Deliverable or Milestone based on a monthly basis for that work completed during the month.
2. Contractor staff must work, at a minimum, during normal core business hours Monday through Friday, except for State holidays. It is the Contractor's responsibility to ensure staff is working within these parameters and to communicate to the State when exceptions, such as requested time off, personal illness or emergencies arise, to ensure these situations will not impact the project or service.
3. Contractor staff work location will be identified in the SOW. If it is not necessary for Contractor staff to be onsite, the Contractor will be responsible for providing an offsite work location. For Work that requires the Contractor to work onsite, the State will provide each Contractor staff workspace and internet access. Contractor personal computing equipment, printers, general office supplies and other administrative items required to perform the work for the State are the sole responsibilities of the Contractor unless the State provides written approval of items to the Contractor.

### 3.8. Currently Identified Work and Enhancement Requirements

The following is an **illustrative listing** of potential BI / Data Warehouse Project requirement areas:

Requirement Group	Major Activities	Timing
1. Major System Upgrades	<ul style="list-style-type: none"> <li>Subsequent BI / Data Warehouse releases within period of performance as made available by PeopleSoft, IBM (DataStage and Cognos), Tableau and other BI Data Warehouse OEM software and hardware providers at the State's preference</li> <li>Support of On-Boarding of New Agency Applications as a result of Projects</li> </ul>	<ul style="list-style-type: none"> <li>As released by BI / Data Warehouse inclusive of Major, Minor, Enhancements</li> </ul>
2. Monthly and Minor Enhancements	<ul style="list-style-type: none"> <li>Monthly within period of performance as made available by PeopleSoft, IBM (DataStage and Cognos), Tableau and other BI Data Warehouse OEM software and hardware providers at the State's preference</li> </ul>	<ul style="list-style-type: none"> <li>As requested under discretionary hours pool</li> </ul>
3. New Agencies	<p><b>Utilizing OIT Established BI / Data Warehouse Standards, Tools, Methods and Capabilities:</b></p> <ul style="list-style-type: none"> <li>Department of Administrative Services -OAKS</li> <li>Ohio Department of Transportation</li> <li>Ohio Bureau of Worker's Compensation</li> <li>Ohio Department of Medicaid</li> <li>Other Agencies determined by the State</li> </ul>	<p>As Agencies onboard over the course of Fiscal Years 2016 – 2018, initially:</p> <ul style="list-style-type: none"> <li>OAKS (Ongoing)</li> <li>Bureau of Workers Compensation (ongoing)</li> <li>Ohio Department of Medicaid (ongoing)</li> <li>ODOT (Summer 2017 and Summer 2018)</li> </ul>
4. New Applications	<p>New Deployments (Update and Maintain) - Additional Capabilities and Modules at the State's request shall be addressed under an mutually agreeable change request, but <b>may</b> include:</p> <ul style="list-style-type: none"> <li>BI / Data Warehouse Operations Management</li> <li>BI / Data Warehouse Automation Platform</li> <li>BI / Data Warehouse Service Management</li> <li>BI / Data Warehouse Business Management</li> </ul>	<p>July 2016 through Contract Conclusion based on State need.</p>

### 3.9. Agency Adoption of the OIT BI / Data Warehouse Platform

Should the Contractor be engaged by any State Agency to perform services using the DAS/OIT BI / Data Warehouse platform as a result of any agreement arising from this RFP, the Contractor will adhere to the project delivery, management, development, testing and deployment conventions contained in this Supplement in such a manner as to drive consistent development, roadmap, project management, operational and maintenance processes to be aligned with and follow the conventions established by DAS/OIT and detailed in this Supplement unless otherwise agreed to in writing by DAS/OIT.

## 4.0 Knowledge Transfer and Educational Services

### 4.1. Overview

Contractor will design and provide the State a formal Knowledge Transfer and Education Service in connection any Major Release of BI / Data Warehouse or six months preceding the expiration or termination of the contract arising from this RFP.

### 4.2. Periodic/Ongoing Knowledge Transfer and Training

In addition, on a continuous basis, the Contractor will conduct informal information sharing and knowledge transfer services coincident with the “go-live” of any mutually defined release of Contractor developed functionality in such a manner as to ensure that State personnel assigned to support, develop, manage or operate the BI platform are apprised of the contents of each release, features, functions, known defects and workarounds and other information as to manage and communicate to DAS/OIT leadership (in general) and users of the system (specifically) as to the most effective use of the then current system assets (i.e., the BI / Data Warehouse platform and Contractor developed enhancements or extensions).

### 4.3. Change Management/Communications and User Training

Over the course of an implementation, the Contractor will have the following responsibilities with regard to the effort which are additive to the general responsibilities contained in this Supplement as they pertain to Change Management and User Training. Each will be discussed in turn:

#### Change Management/Communications

- Contractor will work with the State to develop general communications materials regarding the scope, anticipated impact of change with regard to the contents of a release to the Contractor provided solution(s). These communications documents must be focused (at a minimum) on general communicate to service delivery staff and State expert BI / Data Warehouse users (generally less than 10) for onward dissemination to service delivery teams and OIT customers by the State;
- For expert BI / Data Warehouse Users, the Contractor will develop progress and design summaries to be shared by the State with these users; and
- ★ For the OIT and OAKS service owners that support Agency customers and BI / Data Warehouse help desks, the Contractor will develop targeted presentations that highlight specific system support processes, workflows, job aids and updates arising from the solution implementation.

#### User Training Responsibilities

- ★ For Statewide and Expert Users, the Contractor will develop for the State to publish general guides containing FAQ, one-page “how to” and help pages for the BI / Data Warehouse website on utilizing the new system for required functions; and
- ★ For the State Service delivery functions and Business support functions pertinent to the BI / Data Warehouse the Contractor will develop targeted training sessions as appropriate to Business, Operations (e.g., State IT personnel) and Technical (e.g., State developers or infrastructure personnel) to be delivered that highlight the implementation, use, changes, workflow, reporting and other use considerations in such a manner as to facilitate the migration of business and technical infrastructure support functions to the new system.

#### 4.4. Contract Conclusion Knowledge Transfer and Training

These services shall be designed and delivered in a manner as to (a) to the extent requested by the State, the continued performance by Contractor of its obligations under the Contract (including providing the Services which are subject to termination or expiration), and (b) the provisioning of such assistance, cooperation and information as is reasonably necessary to help enable a smooth transition of the applicable Services to the State or its designated 3<sup>rd</sup> Party provider (“Successor”). As part of these services, Contractor will provide such information as the State may reasonably request relating to features, functions, extensions, configurations, release and programmer notes, FAQs and other delivery artifacts required to operate and maintain the system, and Contractor will make such information available to the State in a Microsoft SharePoint site provided by the State for this purpose.

#### 4.5. Cooperation with State or Successor Contractor

Contractor will cooperate with the State in its attempts at transferring the services responsibilities to another provider in a manner in keeping with not adversely affect the provision of ongoing services.

In addition to the requirements in this section, at the written request of the State, the Contractor will design and deliver a training program (via an approved Statement of Work) to State employees or contractors designed to convey operational and technical knowledge associated with the ongoing operation of the system and systems, conduct knowledge and documentation transfers for the then current operational processes and tasks and work to ensure an overall continuity of services until such time as State employees or contractors can reasonably perform the roles in keeping with service levels and other operational quality, timeliness and accuracy considerations associated with the delivery of the system.

## 5.0 Project Requirements: Applies to All Project Implementation Based Work Contained in this Supplement

### 5.1. Project Management and Coordination Services

The Contractor will, in conjunction with an authorized Statement of Work arising from this RFP:

- Be responsible for the coordination and delivery of overall Project;
- Maintain the overall Project Plan;
- Ensure deliverables have a detailed project sub plan as required by the State to ensure timely delivery and appropriate quality;
- Ensure that all efforts have an effective version control mechanism for all documents within the project document library that will be maintained on a State provided Microsoft SharePoint site;
- Ensure that an appropriate “Project Kickoff” occurs and that all integrated work plans are agreed to by the State from project commencement;
- Complete status reporting adhering to the PMO policies;
- Work with the State leadership to ensure that the Project is staffed appropriately;
- Ensure that required testing activities across both technical and operational components are completed to minimize Project risk; and
- Collaborate with the task areas to ensure appropriate cross-team communication and delivery.

### 5.2. Create and Maintain Project Plan

The Contractor must produce a detailed Project Plan, in electronic and paper form, to the Project Representative (e.g., State’s Project Manager) for approval within twenty business days after the State issues a purchase order or other written payment obligation under the Contract. The Contractor must lead a planning session which ensures the following:

- A common understanding of the work plan has been established;
- A common vision of all deliverables has been established;
- Contains a critical path that identifies all major milestones, dependences (both internal and external to the project), resources by name and resource assignments and is complete and inclusive of the entire work effort from commencement until conclusion of all contracted activities; and
- Clarity on scope of overall project and the responsibilities of the Contractor has been defined and agreed to by the State.

Thereafter, the Contractor must:

- Formally update the Project Plan, including work breakdown structure and schedule, and provide the updated Project plan as part of its reporting requirements during the Project; and
- Ensure the Project Plan allows adequate time and process for the development for the State’s review, commentary, and approval.

The State will determine the number of business days it needs for such reviews and provide that information to the Contractor after award and early in the development of the Project Plan. Should the State reject the plan or associated deliverables, the Contractor must correct all deficiencies and resubmit it for the State’s review and approval until the State accepts the Deliverable at no additional cost to the State.

### 5.3. Meeting Attendance and Reporting Requirements.

The Contractor's project delivery approach must adhere to the following meeting and reporting requirements:

- Immediate Reporting - The Contractor's Project Manager or a designee must immediately report any Project staffing changes to the State BI Team Leader;
- Attend Weekly Status Meetings - The State and Contractor Project Managers and other Contractor Project team members must attend weekly status meetings with the State BI Team Leader and other members of the State Project teams deemed necessary to discuss Project issues. These weekly meetings must follow an agreed upon agenda and allow the Contractor and the State to discuss any issues that concern them;
- Provide Weekly Status Reports - The Contractor must provide written status reports to the Project Representative at least one full business day before each weekly status meeting;
- At a minimum, weekly status reports must contain the items identified below:
  - Updated GANTT chart, along with a copy of the corresponding Project Plan files (i.e. MS Project) on electronic media acceptable to the State;
  - Status of currently planned tasks, specifically identifying tasks not on schedule and a resolution plan to return to the planned schedule;
  - Issues encountered, proposed resolutions, and actual resolutions;
  - Anticipated tasks to be completed in the next week; and
  - Task and Deliverable status, with percentage of completion and time ahead or behind schedule for tasks and milestones.

### 5.4. Utilize OIT's Document Sharing/Collaboration Capability

In conjunction with the delivery of the Project, coincident with the start of the Project through its conclusion, the Contractor must use the State provided and hosted document management and team collaboration capability (Microsoft® SharePoint™) to provide access through internal state networks and secure external connections to all project team members, approved project stakeholders and participants. In conjunction with the utilization of this tool, the Contractor must:

- Structure the document management and collaboration pages and data structures in such a manner as to support the overall requirements of the Project;
- Be responsible for the maintenance and general upkeep of the designer configurations of the tool in keeping with commercially reasonable considerations and industry best practices as to not adversely impact the project delivery efforts performed by the Contractor and State; and
- At the conclusion of the project, or upon request of the State, ensure that the State is provided a machine readable and comprehensive backup of the SharePoint™ database(s) contained within the tool that is owned by the State and not proprietary to the Contractor or otherwise required by the State to maintain ongoing project documentation and artifacts (i.e., Contractor is to remove all Contractor proprietary or non-State owned or licensed materials from the tool).

### 5.5. System and Acceptance Testing Requirements

For any BI / Data Warehouse Major/Minor Upgrades, Technical Implementation, code-based deliverables, development, upgrade / update or elements will be subject to a formal testing and acceptance process that uses objective and thorough test criteria established by the Parties that will allow the Parties to verify that each build meets the specified functional, technical and where appropriate, performance requirements. The testing and

acceptance process will be developed for each build as soon as possible after establishing the business and user requirements. The testing and acceptance process will include sufficient audit trails and documentation as required to track and correct issues.

The tasks and activities that the Contractor will perform as part of the testing and acceptance process include the following:

- Develop and maintain test data repositories as agreed appropriate;
- Develop test plans, scripts, cases and schedules as agreed appropriate;
- Perform the following testing activities for solution components and assess quality and completeness of results including:
  - System Test / Assembly;
  - Integration/interface testing and regression testing for new releases of existing applications; and
  - Performance Test including regression testing new releases of existing applications as well as the potential performance impacts to current production environments where a risk of impacting performance may be introduced as a result of these elements;
- Provision test environments populated with quasi production data as required to perform the system and user acceptance testing work, and where appropriate performance testing. The test environments will be designed and maintained by Contractor so that test activities will not adversely affect the production environment. Contractor will expand capacity if testing requirements are constrained by the hardware; and
- ★ Document system and performance test results for State review and acceptance prior to the State's commencement of acceptance testing.

## 5.6. Support the State's Performance of User Acceptance Test (UAT)

The Contractor will support the State's user acceptance testing for solution components as follows:

- Develop with the State agreed upon UAT test plans, scripts, cases and applicable acceptance criteria;
- Coordinate UAT execution and acceptance procedures with the appropriate the State participants;
- Record and report UAT results;
- Review changes, fixes and enhancements with the participants in the UAT testing;
- Correct identified defects and nonconformities in accordance with the acceptance process;
- Compile and maintain solution issue lists;
- Coordinate and confirm the State approval of solution components and verification of applicable acceptance criteria for transition into deployment and production use; and
- Provide the State with reports on a weekly basis tracking the progress of Contractor's performance of testing work, or in the case of user acceptance testing, support of the State activities. In addition, Contractor will provide timely responses to the State's requests for information and reports necessary to provide updates to the State business units and stakeholders. Contractor will also provide the State with a database extract from the database that tracks progress of Contractor's performance of testing work.

## 5.7. Pre-Production / Production Deployment Phase

The Contractor will be responsible for working with the State and its 3<sup>rd</sup> party contractors, and executing the production deployment and roll-out of any BI / Data Warehouse Technical Implementation to the Production Environment(s) utilized by the State.

Contractor will comply with the State required implementation and deployment procedures. This may include, network laboratory testing, migration procedures, the use of any pre-production or pseudo-production environment prior to production migration. Contractor will be responsible for business user support required during the initial weeks of a production deployment as determined by the affected State business units and will maintain the capability to provide enhanced levels of support during the term of the Contract. Contractor will submit to the State, for the State's approval, a written deployment plan describing Contractor's plan to manage each such implementation, including working with the State's Infrastructure Services Division, if applicable.

The tasks and activities to be performed by Contractor as part of the Deployment Services also include the following:

- Execute required data conversions or migrations including, but not limited to, baseline BI / Data Warehouse configuration tables and parameters, and ancillary supporting data as required by the system to function successfully in the production environment;
- Establish data to be used with the new solution by producing new data and reconciling and mapping different data and database representations;
- If required, convert electronic data into a format usable by the new solution using a data conversion program;
- Document data issues and provide to the State for resolution;
- Conduct production pilot(s) (including "day in the life" simulations) and fine tune solution as agreed appropriate;
- End to end final validation of the operational architecture for the system;
- Develop, and thereafter maintain and make available to the State, a knowledge base of documentation gathered throughout the Project's life and allow for re-use of such documentation for future Projects; and
- Conduct a post-implementation review process upon the completion of the Project which will include an analysis of how the business system(s) resulting from the Project compare to the post-deployment performance requirements established for such Project.

## 5.8. System Changes as a Result of Contractor Projects

For those System Changes (updates, upgrades, patches or otherwise) to any State system or environment within the Contractor's scope of work that involve the change of code or data (BI / Data Warehouse, Interfaces, Scripts, Web Pages, Database Structures/Elements, operating system or database scripts, extensions, configuration items or otherwise) associated with the Contractor's effort, the Contractor will:

- Support the State to establish, publish and maintain a formal release calendar in consideration of the scheduled or required changes to the BI system;
- Support the State in the development of release packaging rules that include provisions for Contractor system and performance testing, State review and approval of Contractor results, provisions for State acceptance or validation testing (depending on the nature of the change);
- Operational procedures to backup or otherwise copy the BI / Data Warehouse environment prior to implementing the change; and
- Rollback or reversibility considerations including success/failure criterion applicable to the change.

The Contractor will implement, utilize and maintain:

- Structured code management, version control tools based on a supported change management suite;

- Include requirements traceability for all elements of a system change;
- Ensure that all changes adhere to State security, privacy and data handling Policies as contained in Supplement 2;
- Employ standard test beds or scripts that are utilized and extended for purposes of fully demonstrating completeness of adherence to business, functional and technical requirements at State required quality levels; and
- If applicable, include performance testing for high volume (transaction or data) transactions at the mutual agreement of the State and Contractor in consideration of the contents of a change.

## 5.9. Project Completion Activities and Final Documentation Handoff

Following forty-five (45) days of successful execution (defined as no Severity 1 or 2 issues) by the Contractor to the State production environment, the Contractor shall be relieved of Project requirements contained herein. During the 45 day period immediately following the introduction of the Contractor provided enhancements, configurations or extensions to the State’s production environment the Contractor must:

- Ensure adequate staffing from the Contractor Project Team is on hand (or available remotely) to ensure that during this 45 day period all defects identified by the State and mutually committed to be resolve by the Contractor in this RFP or under any SOW are adhered to.
- This responsibility shall specifically include:
  - Prompt isolation, triage and repair of any Severity 1 or 2 issues;
  - Performance Monitoring of the System to ensure that there are no statistically significant (i.e., +5%) deviations from actual production performance as compared to the system performance prior to the implementation of Contractor developed elements;
  - All interfaces, and system functions perform and function as specified; and
  - Compile all final versions of the upgrade documentation, work products and delivery materials and locate / organize them as ‘FINAL’ on the State provided SharePoint site.
- ★ Obtain a final acceptance document from the State and the Contractor Managed Service Team confirming that all of the above has been delivered and accepted as final.

If, during the 45 day period immediately following the introduction to Production, a Severity 1 or 2 issue occurs that can be directly attributable to the efforts of the Contractor, and not the State, or other non-Project parties, the 45 day period will, at the sole discretion of the State, be reset for additional 45 day periods until such time as the system can perform without Severity 1 and 2 issues.

An Incident shall be categorized as a “Severity 1 Outage” if the Incident is characterized by the following attributes: the Incident (a) renders a business critical System, Service, Software, Equipment or network component un-Available, substantially un-Available or seriously impacts normal business operations, in each case prohibiting the execution of productive work, and (b) affects either (i) a group or groups of people, or (ii) a single individual performing a critical business function.

“Severity 2 Outage” is defined as : An Incident shall be categorized as a “Severity 2 Outage” if the Incident is characterized by the following attributes: the Incident (a) does not render a business critical System, Service, Software, Equipment or network component un-Available or substantially un-Available, but a function or functions are not Available, substantially Available or functioning as they should, in each case prohibiting the execution of productive work, and (b) affects either (i) a group or groups of people, or (ii) a single individual performing a critical business function.

## 6.0 Required Contractor Roles, Minimum Standards

### 6.1. Operational Run Roles and Staffing

The Offeror will provide below the proposed staffing (roles and table of organization) offered to support **Operational Run** requirements and responsibilities as contained in Sections 2, 4 and 8 in their entirety:

The offeror is to consider the roles proposed that are required at a minimum for any Run Service based upon the details, the key activities, proposed time commitments required for each role, and the percent of the proposed time the role will be on the State’s premises performing work. The offeror, as part of their response will identify all roles that are required to be performed (by work area), the work location(s) for the team and identify requirements for performing these roles off-site at a Contractor location or on State’s Premises (e.g., Operations Manager, business analysis, technical lead, functional lead, etc.).

#### Offeror Team Organization at a minimum, Key Personnel and Work Location(s) – Run Services

Role #	Contractor Role	Role Activity	Key Personnel	% Time On Site
<b>Operations, Maintenance and Run Services: Lead/Management</b>				
1	<b>Operations Manager</b>	<ul style="list-style-type: none"> <li>Eight (8) years' experience with managerial level operational activities, business analysis, manage Project issues and risks, drive timely resolution, preferably on ERP and/or (BI) business intelligence projects through full SDLC. Seek State approvals from State BI Team leader.</li> <li>Experience in Public Sector is preferred (Federal, State, Local/Municipal Government or Higher Education Preferred).</li> </ul>	Yes/ Provide Name and Resume	80%
2	<b>Business Analyst</b>	<ul style="list-style-type: none"> <li>Bachelor's Degree, MBA Preferred. Multiple years' experience in communicating effectively, liaison between customer and developers, assist in presentations, change preparedness initiatives. Experience in BI operations preferred. Excellent oral and written communication. Co-ordinates prioritization with State BI Team Leader.</li> <li>Experience in Public Sector is preferred (Federal, State, Local/Municipal Government or Higher Education Preferred).</li> </ul>	Yes/ Provide Name and Resume	80%
<b>Operations, Maintenance and Run Services: Technical (ETL, Cognos, Database, etc.)</b>				
3	<b>ETL Developer</b>	<ul style="list-style-type: none"> <li>Five years' experience developing and maintaining ETLs using IBM InfoSphere DataStage (v 8.5 preferred). Sourcing from tables, files, break fixes, UC4 etc. Prefer PeopleSoft EPM experience. Demonstrated technical documentation skills</li> <li>Experience in Public Sector is preferred (Federal, State, Local/Municipal Government or Higher Education Preferred).</li> </ul>	Yes/ Provide Name and Resume	80%
4	<b>Cognos Developer/Admin</b>	<ul style="list-style-type: none"> <li>Five years' experience in Cognos Product. Performs SDLC activities for Projects that include Cognos including development and maintenance of metadata and all types of Business Intelligences on behalf of the BI Organization. Develops BI metadata models on top of EPM Data marts, Dashboards/reports and Cognos Administration</li> <li>Experience in Public Sector is preferred (Federal, State, Local/Municipal Government or Higher Education Preferred).</li> </ul>	Yes/ Provide Name and Resume	80% On call during nightly batch.
<b>Operations, Maintenance and Run Services: Functional &amp; Other Support Roles</b>				

Role #	Contractor Role	Role Activity	Key Personnel	% Time On Site
5	Trainer	<ul style="list-style-type: none"> <li>Five years' experience in Cognos Product. Five years' experience in training in Cognos, Tableau and BI environments and data marts (GL, HCM, FIN, ELM etc.) and course outlining skills.</li> <li>Experience in Public Sector is preferred (Federal, State, Local/Municipal Government or Higher Education Preferred).</li> </ul>	Yes/ Provide Name and Resume	80%

## 6.2. BI Project Roles and Capabilities

The Offeror will provide resumes for following roles at a minimum to support BI Project delivery requirements and responsibilities as contained in Sections 3, 4, 5 and 9 in their entirety to demonstrate the capabilities of the firm and Project Personnel assigned to State projects. Offerors are to note that the actual team composition, skills, staffing levels and duration for Project Personnel will be determined by mutual agreement with the State, dependent on specific needs of a Project under a State approved IDA.

Position / Capability	Basic Qualifications
<b>Business Intelligence Project Manager</b>	<p>Eight years' experience with managerial level operational activities, business analysis, preferably on ERP and/or business intelligence projects through full SDLC. Multi-module PeopleSoft experience. Project management experience – planning and communications with all internal and external partners to deliver successful Projects and Agency Engagements in accordance with State requirements.</p> <p>Demonstrated Ability to:</p> <ul style="list-style-type: none"> <li>Work with the BI and Agency Project Managers to create and manage the Project Plan and Schedule</li> <li>Manage the Contractor Project Team Members</li> <li>Manage overall quality and timeliness of the Project deliverables</li> <li>Manage Project issues and risks</li> <li>Function as Point of escalation and resolution for Project issues</li> </ul> <p>Experience in Public Sector (Federal, State, Local/Municipal Government or Higher Education Preferred).</p>
<b>Business Lead(s)</b> – Based on Project portfolio, multiple roles may be required as determined by the State	<p>Five years' experience in business analysis, preferably on ERP and/or business intelligence projects through full SDLC. Multi-module PeopleSoft experience. Expertise in common BI schemas, Oracle DBMS functionality and features, and tuning techniques.</p> <p>Demonstrated Experience and Ability to:</p> <ul style="list-style-type: none"> <li>Manage design, development, testing and implement of Business Intelligence and management reporting functionality</li> <li>Manage deployment of BI tool training and data model training to BI power users prior to system go-live for each deployment phase</li> <li>Coordinate activities in the BI area with Contractor team and the OAKS and Agency Project Managers and State BI Team Leader through completion of the Project.</li> <li>Work with the Contractor team, BI and Agency Business Owners and State BI Team Leader on project activities in the BI area</li> <li>Manage the Contractor project team members (functional and technical) in a BI project</li> </ul> <p>Experience in Public Sector (Federal, State, Local/Municipal Government or Higher Education Preferred).</p>

Position / Capability	Basic Qualifications
<p><b>Cognos Developer(s)</b>– Cognos Development for full lifecycle projects (Analysis, Design, Construction and Deployment)</p> <p>Based on Project portfolio, multiple roles may be required as determined by the State</p>	<p>Five years' experience in Cognos Product. Performs SDLC activities for Projects that include Cognos including development and maintenance of metadata and all types of Business Intelligences on behalf of the BI Organization. Develops BI metadata models on top of EPM Data marts, Dashboards/reports and Cognos Administration</p>
<p><b>Tableau Developer(s)</b>– Tableau Development for full lifecycle projects (Analysis, Design, Construction and Deployment)</p> <p>Based on Project portfolio, multiple roles may be required as determined by the State</p>	<p>Demonstrated experience in Tableau Product. Performs SDLC activities for Projects that include Cognos including development and maintenance of metadata and all types of Business Intelligences on behalf of the BI Organization. Develops BI metadata models on top of EPM Data marts, Dashboards/reports and Tableau best practices</p>
<p><b>Business Analyst/Organizational Change Management Analyst(s)</b></p> <p>Based on Project portfolio, multiple roles may be required as determined by the State</p>	<p>Bachelor's Degree, MBA Preferred. Multiple years' experience in communicating effectively, liaison between customer and developers, preparing mass messages, presentations, trainings, change preparedness initiatives. Excellent oral and written communications skills (Word, Visio, PowerPoint).</p> <p>Experience in Public Sector (Federal, State, Local/Municipal Government or Higher Education Preferred).</p>
<p><b>Trainer(s)</b> – 80% allocation to training and 20% allocation to supporting change activities.</p> <p>Based on Project portfolio, multiple roles may be required as determined by the State</p>	<p>Five years' experience in training in Cognos, Tableau and BI environments and data marts (GL, HCM, FIN, ELM etc.) and course outlining skills.</p> <p>Experience in Public Sector (Federal, State, Local/Municipal Government or Higher Education Preferred).</p>
<p><b>ETL Developer(s)</b> –ETL design and development.</p> <p>Based on Project portfolio, multiple roles may be required as determined by the State</p>	<p>Five years' experience developing and maintaining ETLs using IBM InfoSphere DataStage (v 8.5 preferred). Sourcing from tables, files, break fixes, UC4 etc. Prefer PeopleSoft EPM experience. Demonstrated technical documentation skills.</p>

### 6.3. Staffing and Time Commitment (Operational Run and Project Services)

The offeror must include a statement indicating to what extent, if any, the candidates may work on other projects or assignments that are **not** related to this Contract during the term of the Contract. The State may reject any Proposal that commits the proposed Project Manager or any proposed Key Personnel to other projects during the term of the Project, if the State believes that any such commitment may be detrimental to the offeror's performance.

In addition, the offeror's proposal must identify all Key Personnel as listed in the preceding table who will provide services as part of the resulting Contract. The Key Personnel are identified in each applicable Supplement. The State expects that the proposed named Key Personnel will be available as proposed to work on the Project. Resumes for the proposed candidates must be provided for all Key Personnel. Representative resumes are **not** acceptable. The resumes will be used to supplement the descriptive narrative provided by the offeror regarding their proposed project team.

The resume (2-page limit per resume) of the proposed Key Project Personnel must include:

- Proposed Candidate's Name

- Proposed role on this Project
- Listings of completed projects (a minimum of two references for each named Key Project Personnel) that are comparable to this Project or required similar skills based on the person's assigned role/responsibility on this Project. Each project listed should include at a minimum the beginning and ending dates, client/company name for which the work was performed, client contact information for sponsoring Directors, Managers or equivalent level position (name, phone number, email address, company name, etc.), project title, project description, and a detailed description of the person's role/responsibility on the project.
- Education
- Professional Licenses/Certifications/Memberships
- Employment History

The State desires a team whose members have previous experience working together on past projects. Offerors must provide information regarding any past experience where team members worked on previous projects together.

## 7.0 Assumptions, Staffing and Support Requirements, Commercial Materials and Other Matters

The Offeror must list all the assumptions the Offeror made in preparing the Proposal. If any assumption is unacceptable to the State, the State may at its sole discretion request that the Offeror remove the assumption or choose to reject the Proposal. No assumptions may be included regarding the outcomes of negotiation, terms and conditions, or requirements. Assumptions should be provided as part of the Offeror response as a stand-alone response section that is inclusive of all assumptions with reference(s) to the section(s) of the RFP that the assumption is applicable to. **Offerors should not include assumptions elsewhere in their response, for the avoidance of doubt, all Offeror assumptions must be contained in this section and assumptions contained elsewhere may not be considered valid by the State.**

### 7.1. Support Requirements

The Offeror must describe the support it wants from the State other than what the State has offered in this RFP. Specifically, the Offeror must address the following:

- Nature and extent of State support required in terms of staff roles, percentage of time available, and so on;
- Assistance from State staff and the experience and qualification levels required; and
- Other support requirements.

The State may not be able or willing to provide the additional support the Offeror lists in this part of its Proposal. The Offeror therefore must indicate whether its request for additional support is a requirement for its performance. If any part of the list is a requirement, the State may reject the Offeror's Proposal, if the State is unable or unwilling to meet the requirements.

### 7.2. Pre-Existing Materials

The Offeror must list any Pre-Existing Materials it owns that will be included in a Deliverable if the Offeror wants a proprietary notice on copies that the State distributes. For example, the Offeror may have standard user interfaces or standard shells that it incorporates in what is otherwise custom software. (See the Ownership of Deliverables section of the General Terms and Conditions.) The State may reject any Proposal that includes existing materials for a custom solution, if the State believes that such is not appropriate or desirable for the Project.

### 7.3. Commercial Materials

The Offeror must list any commercial and proprietary materials that the Offeror will deliver that are easily copied, such as Commercial Software, and in which the State will have less than full ownership ("Commercial Materials"). Generally, these will be from third parties and readily available in the open market. The Offeror need not list patented parts of equipment, since they are not readily copied. If the Offeror expects the State to sign a license for the Commercial Material, the Offeror must include the license agreement as an attachment. If the State finds any provisions of the license agreement objectionable and cannot or does not negotiate an acceptable solution with the licensor, regardless of the reason and in the State's sole discretion, then the Offeror's Proposal may be rejected. If the State is not going to sign a license, but there will be limits on the State's use of the Commercial Materials different from the standard license in the General Terms and Conditions, then the Offeror must detail the unique scope of license here. Unless otherwise provided in this RFP, proposing to use Commercial Materials in a custom solution may be a basis for rejection of the Offeror's Proposal, if the State, in its sole discretion,

believes that such is not appropriate or desirable for the Project. Any deviation from the standard license, warranty, and other terms in Attachment Four also may result in a rejection of the Offeror's Proposal.

If the Offeror proposes a Deliverable that contains Commercial Software or other Commercial Materials with terms that differ from the terms in Attachment Four for Commercial Software and Materials, then those terms must be detailed here, and any proposed separate agreement covering those items must be included in the Offeror's Proposal. This is required even if the State will not be expected to sign the agreement. Any deviation from the standard terms in Attachment Four may result in a rejection of the Offeror's Proposal.

#### 7.4. Personnel Considerations

In an effort to foster a mutually supportive and collaborative environment in which the Services are provided in an effective manner that drives value to the State of Ohio, the Parties will jointly review the performance of certain Key Contractor Management and State Facing positions (collectively "Key Personnel", including the Contractor Account Representative. "Key Personnel" will include the following at a minimum:

- Contractor Account Representative
- Managed Services Delivery Team personnel performing Services on State Premises
- Managed Services Delivery Team personnel that have regular (i.e., more than 50% of their productive time) spent in direct interaction with State personnel (i.e., face-to-face or remotely via teleconference or phone calls)
- Function Leads (e.g., EPM/BI) and Production/Change Management Leads (e.g., operations, production control, L 2/3 Service Desk)
- Applicable Major Project Stream or Tower Leads for Contractor led Major Projects
- Other Contractor Personnel as Mutually Agreed

Based on the State of Ohio's experience with BI and similar managed services relationships with a variety of vendors, the State of Ohio feels strongly that the Contractor team (as a team and as individuals) should be regularly reviewed with regard to several key factors including, but not limited to:

- Support of State BI initiatives including Agency adoption of BI and Data Warehouse Consolidation;
- Attainment of high customer satisfaction in Stakeholder (i.e., DAS, OBM, GSD and Agency) communities and by extension and importantly end-user communities;
- Creation of a highly integrated, collaborative and mutually supportive delivery of Services under this SOW to the State of Ohio through the formation of an "integrated team" culture;
- Adoption, implementation and refinement of a "State First" operating culture that is designed to drive value through the relationship and result in a high-performance working partnership between the State of Ohio and Contractor;
- Incorporation of industry-leading and Contractor best practices in the construction, operation, maintenance and support of BI while seeking opportunities for continuous refinement and improvement of areas that are directly within the Contractor's scope, those areas where the Contractor has a reliance on the State of Ohio and 3rd parties, and areas in the common interest of driving Service efficiency, quality and timeliness (e.g., Value).

The State of Ohio and Contractor will meet on a regular basis, no less frequently than annually, to review the Contractor's performance (as a team and as individuals) in support of these goals and agree to make changes to the number, nature, mix or named Key Personnel as required to improve and enhance the Contractor's position in supporting the State of Ohio's attainment of these goals. As a one-time evaluation the Contractor and State shall meet to review the performance of the entire Contractor team within 90 days of completion of Transition activities as required herein and implement any changes so that the Service is launched on the best possible Contractor team as possible.

Should, for whatever reason, the State of Ohio determine based on documented or observed performance that a member (or members) of the Contractor's Key Personnel is operating in a manner inconsistent with these Goals, the State of Ohio will request a meeting of the Contractor Account Representative and the OAKS Administrator (and if required the State of Ohio CIO and Contractor Managing Director or Lead Partner for Public Sector) to address localized or endemic failures to meet these goals. Upon receiving this feedback, the Contractor will develop and implement a plan to either realign the performance of the Key personnel in question or replace them promptly should the situation dictate in accordance with the provisions of this RFP pertaining to Replacement Personnel.

For the avoidance of doubt, should for whatever reason the State of Ohio OAKS Administrator request the replacement of any member of the Contractor Staff, the Contractor shall implement the change on a mutually agreeable schedule.

Should, for any reason described above the State of Ohio and Contractor determine that a member of the Contractor Key Personnel need replacement, this replacement shall occur no later than thirty (30) calendar days from the State of Ohio's request or as agreed.

Additionally, the Contractor will provide a listing no less frequently than monthly, a report to the State of Ohio of Contractor personnel associated with the performance of the work contained in this Supplement by identified role, Key Personnel or otherwise (e.g., Account Representative, Operations Lead, Job Scheduler, DBA, etc.) showing total hours and the name of the individual(s) associated with performing the contracted work and roles.

## 7.5. Dispute Resolution

### Informal Dispute Resolution

Prior to the initiation of formal dispute resolution procedures as to any dispute (other than those arising out of the breach of a Party's obligations), the Parties will first attempt to resolve each dispute informally, as follows:

- If the Parties are unable to resolve a dispute in an amount of time that either Party deems required under the circumstances, such Party may refer the dispute to the State CIO or designee by delivering a written notice of such referral to the other Party.
- Within five (5) Business Days of the delivery of a notice referring a dispute to the State CIO or designee, each Party will prepare and submit to the Managed Services Oversight Council a detailed summary of the dispute, the underlying facts, supporting information and documentation and their respective positions, together with any supporting documentation.
- The State CIO or designee will address the dispute at its next regularly scheduled meeting or, at the request of either Party, will conduct a special meeting within ten (10) Business Days to address such dispute. The State CIO or designee will address the dispute in an effort to resolve such dispute without the necessity of any formal proceeding.
- The State CIO or designee will address the dispute at the next regularly scheduled meeting between the Contractor and the State or, at the request of either Party, will conduct a special meeting within twenty (20) Business Days to address such dispute. The State CIO or designee will address the dispute in an effort to resolve such dispute without the necessity of any formal proceeding.
- If the State CIO or designee is unable to resolve a dispute within thirty (30) days of the first regular meeting between the State and Contractor addressing such dispute (or such longer period of time as the Parties may agree upon), either Party may refer the dispute to internal escalation by delivering written notice of such referral to the other Party.

## Internal Escalation

If for whatever reason the Contractor and the State cannot resolve a dispute via the above escalation processes and procedures, the Contractor and the State agree to choose a mutually agreeable neutral third party who will mediate the dispute between the parties. The mediator chosen must be an experienced mediator and must not be: a current or former employee of either party or associated with any aspect of the Government of the State of Ohio; associated with any equipment or software supplier; or associated with the Contractor or the State. As to each prohibition this means either directly or indirectly or by virtue of any material financial interests, directly or indirectly, or by virtue of any family members, close friendships or in any way that would have the reasonable appearance of either conflict or potential for bias. If the parties are unable to agree on a qualified person, the mediator will be appointed by the American Arbitration Association.

The mediation must be non-binding and must be confidential to the extent permitted by law. Each party must be represented in the mediation by a person with authority to settle the dispute. The parties must participate in good faith in accordance with the recommendations of the mediator and must follow procedures for mediation as suggested by the mediator. All mediation expenses, except expenses of the individual parties, must be shared equally by the parties. The parties must refrain from court proceedings during the mediation process insofar as they can do so without prejudicing their legal rights.

If the disputed matter has not been resolved within thirty (30) days thereafter, or such longer period as agreed to in writing by the Parties, each Party will have the right to commence any legal proceeding as permitted by law.

## Escalation for Repetitive Service Level Failures

Although it is the State's intent to escalate service level failures to the Contractor Account Representative, the State may decide to escalate to other levels within the Contractor's corporate structure deemed appropriate to resolve repetitive service failures.

## 8.0 Service Level Requirements: State BI / Data Warehouse Projects

This section sets forth the performance specifications for the Service Level Agreements (SLA) and Service Level Objectives (SLO) to be established between the Contractor and the State that are applicable to any work associated with the development, configuration, extension or implementation of any software associated with this Supplement in general, and under Section 3.0 specifically as the work pertains to any BI Projects or subsequent or Additional Work for State Agencies.

The section contains the tables and descriptions that provide the State framework, requirements relating to service level commitments, and the implications of meeting versus failing to meet the requirements and objectives, as applicable. This document defines the State's detailed performance, management, and reporting requirements for the Project Implementation Project and to all subsequent Project related services and phases that are contracted under future Statements of Work between the State and the Contractor related to this RFP.

The mechanism set out herein will be implemented to manage the Contractor's performance against each Service Level, in order to monitor the overall performance of the Contractor.

The Contractor will be required to comply with the following performance management and reporting mechanisms for all Services within the scope of this RFP and will provide these reports to the State on a no less frequent than monthly basis:

- **Service Level Specific Performance** – Agreed upon specific Service Levels to measure the performance of specific Services or Service Elements. Most individual Service Levels are linked to financial credits due to the State ("Performance Credits") to incent Contractor performance.

- **Overall Contract Performance** – An overall performance score of the Contractor across all Service Levels. The overall performance score is linked to governance and escalation processes as-needed to initiate corrective actions and remedial processes.

### 8.1. Service Level Specific Performance Credits

Each Service Level (SL) will be measured using a “Green-Yellow-Red” traffic light mechanism (the “Individual SL GYR State”), with “Green” representing the highest level of performance and “Red” representing the lowest level of performance. A Performance Credit will be due to the State in the event a specific Individual SLA GYR State falls in the “Yellow” or “Red” state. The amount of the Performance Credit for each SLA will be based on the Individual SLA GYR State. Further, the amounts of the Performance Credits will, in certain cases, increase where they are imposed in consecutive months. No Service Level Performance Credit will be payable for the Contractor’s failure to meet a Service Level Objective.

Set forth below is a table summarizing the monthly Performance Credits for each SLA. All amounts set forth below that are contained in a row pertaining to the “Yellow” or “Red” GYR State, represent Performance Credit amounts.

Consecutive (SLA Performance Credits)												
Individual SL GYR State	1st Month	2nd Month	3rd Month	4th Month	5th Month	6th Month	7th Month	8th Month	9th Month	10th Month	11th Month	12th Month
Red	A =1.71% of MPC	A + 50% of A	A + 100% of A	A + 150% of A	A + 200% of A	A + 250% of A	A + 300% of A	A + 350% of A	A + 400% of A	A + 450% of A	A + 500% of A	A + 550% of A
Yellow	B = 0.855% of MPC	B + 50% of B	B + 100% of B	B + 150% of B	B + 200% of B	B + 250% of B	B + 300% of B	B + 350% of B	B + 400% of B	B + 450% of B	B + 500% of B	B + 550% of B
Green	None	None	None	None	None	None	None	None	None	None	None	None

The Contractor agrees that in each month of the Contract, 12% of the monthly project charges (MPC) associated with the Project Implementation portion of this RFP will be at risk. MPCs are the charges for the deliverables accepted during a given month. The MPC for the Project Implementation will be at risk for failure to meet the Service Levels set forth in the Contract. The Contractor will not be required to provide Performance Credits for multiple Performance Specifications for the same event; the highest Performance Credit available to the State for that particular event will apply.

On a quarterly basis, there will be a “true-up” at which time the total amount of the Performance Credits will be calculated (the “Net Amount”), and such Net Amount will be set off against any fees owed by the State to the Contractor.

Moreover, in the event of consecutive failures to meet the Service Levels, the Contractor will be required to credit the State the maximum Performance Credit under the terms of the Contract.

The Contractor will not be liable for any failed Service Level caused by circumstances beyond its control, and that could not be avoided or mitigated through the exercise of prudence and ordinary care, provided that the Contractor immediately notifies the State in writing and takes all steps necessary to minimize the effect of such circumstances and resumes its performance of the Services in accordance with the SLAs as soon as possible.

For example, if an Individual SL GYR State is Yellow in the first Measurement Period, Red in the second Measurement Period and back to Yellow in the third Measurement Period for an SLA then the Performance Credit due to the State will be the sum of Yellow Month 1 (B) for the first Measurement Period, Red Month 2 (A + 50% of A) for the second Measurement period, and Yellow Month 3 (B + 100% of B) for the third Measurement period, provided (1) such Performance Credit does not exceed 12% of the MPC (the At-Risk Amount); and, (2) no single Service Level Credit will exceed 20% of the total At-Risk Amount, as stated below:

SLA Calculation EXAMPLE						
Monthly Project Charge (MPC) = \$290,000.00						
Monthly At Risk Amount = 12% of MPC = \$34,800						
Maximum for any one SLA = 20% of At Risk Amount = \$6,960						
GYR State	1 <sup>st</sup> Month		2 <sup>nd</sup> Month		3 <sup>rd</sup> Month	
Red	0	\$	0	\$7,438.50	0	
Yellow	1	\$2,479.50	1		1	\$4,959.00
Green	6	\$	6		6	
Totals	7	\$2,479.50	7	\$7,438.50	7	\$4,959.00
Adjusted Totals by At Risk Amount and 20% per individual SLA Limitations	(Is monthly total of all Service Level Credits equal to or less than \$34,800?) - Yes (Is monthly amount for any one Service Level Credit equal to or less than \$ 6,960?) - Yes \$2,479.50		(Is monthly total of all Service Level Credits equal to or less than \$34,800?) - Yes (Is monthly amount for any one Service Level Credit equal to or less than \$ 6,960?) - No \$6,960.00		(Is monthly total of all Service Level Credits equal to or less than \$34,800?) - Yes (Is monthly amount for any one Service Level Credit equal to or less than \$ 6,960?) - Yes \$4,959.00	
Total Quarterly Credit:	\$ 2,479.50 +		\$ 6,960.00 +		\$ 4,959.00	
Total Quarterly Credit: \$ 14,398.50						

Service Level Performance Credit payable to the State = (B) + (A + 50% A) + (B + 100% B), based on an illustrative MPC of \$290,000;

The total of any weighting factors may not exceed 100% of the total At-Risk Amount. To further clarify, the Performance Credits available to the State will not constitute the State’s exclusive remedy to resolving issues related to the Contractor’s performance. Service Levels will commence with Project initiation for any Implementation Project.

## 8.2. Overall Contract Performance

In addition to the service specific performance credits, on a monthly basis, an overall SL score (the “Overall SL Score”) will be determined, by assigning points to each SL based on its Individual SL GYR State. The matrix set forth below describes the methodology for computing the Overall SL Score:

Individual SLAs and SLOs GYR State	Performance Multiple
Green	0
Yellow	1
Red	4

The Overall SL score is calculated by multiplying the number of SLAs and SLOs in each GYR State by the Performance Multiples above. For example, if all SLAs and SLOs are Green except for two SLAs in a Red GYR State, the Overall SL Score would be the equivalent of 8 (4 x 2 Red SLAs).

Based on the Overall SL Score thresholds value exceeding a threshold of fifteen (15), mandatory Executive escalation procedures outlined in this RFP will be initiated to restore acceptable Service Levels.

If a successful resolution is not reached, then **the State may terminate the Contract for cause if:**

The overall SL score reaches a threshold over a period of 3 consecutive months with the equivalent of 50% of the service levels in a red state; and the Contractor fails to cure the affected Service Levels within 60 calendar days of receipt of the State’s written notice of intent to terminate; **OR**

The State exercises its right to terminate for exceeding the threshold level of 75% of Service levels in total over a six (6) month period.

**The Overall Contract Performance will not constitute the State’s exclusive remedy to resolving issues related to the Contractor’s performance. The State retains the right to terminate for Overall Contract Performance under the terms of this Contract.**

### 8.3. Monthly Service Level Report

On a State accounting monthly basis, the Contractor will provide a written report (the “Monthly Service Level Report”) to the State which includes the following information: (i) the Contractor’s quantitative performance for each Service Level; (ii) each Individual SL GYR State and the Overall SL Score; (iii) the amount of any monthly Performance Credit for each Service Level (iv) the year-to-date total Performance Credit balance for each Service Level and all the Service Levels; (v) a “Root-Cause Analysis” and corrective action plan with respect to any Service Levels where the Individual SL GYR State was not “Green” during the preceding month; and (vi) trend or statistical analysis with respect to each Service Level as requested by the State . The Monthly Service Level Report will be due no later than the tenth (10th) accounting day of the following month.

**Failure to report any SLA, SLA performance in a given month, or for any non-Green (i.e., performing to Standard) SLA a detailed root cause analysis that substantiates cause will result in the State considering the performance of the Contractor for that period as performing in a Red State.**

### 8.4. Service Level Commitments – Project Implementation Services

The Contractor will meet the Service Level Commitment for each Service Level set forth in the tables and descriptions below:

Service Level	State Requirements			
	SLA or SLO	Support Hours	Required	
			Response	Resolution
Defect Resolution – Severity 1 Items	SLA	7x24	Every 4 hours until resolution	<= 24 hours
Defect Resolution – Severity 2 Items	SLA	7x16	Every 8 hours until resolution	<=72 hours
Defect Resolution – Severity 3 Items	SLO	5x9	Every 24 hours until resolution	<= 7 calendar days
System Test Execution Exit Quality Rate	SLA	-	See specification below	-
Blocking Issues Identification and Removal	SLA	7x24	Every 2 hours until resolution or agreeable workaround is implemented	<=10%%
Regression Testing Performance Issue Find/Fix Rate	SLA	-	See specification below	-
Code Coverage – Automated Test Beds	SLO	-	See specification below	-
Milestone Date Delivery	SLA	-	See specification below	-
Issue Reporting	SLO	-	See specification below	-
Deliverable Acceptance	SLO	-	See specification below	-
UAT Process and Environment Support	SLO	7x9	Every 2 hours until completion of testing effort	-
Development Methodology Compliance– % SDLC Compliance	SLA	-	See specification below	-
Development Methodology Compliance – % Build and Testing Activities	SLO	-	See specification below	-
Development Methodology Compliance - Issues Detected and Resolved in Production	SLO	-	See specification below	-

## 8.5. Service Level Specifications

### 8.5.1. Defect Resolution – Mean Time to Repair/Resolve (Severity 1 Items)

**Specification:** Defect Resolution – Mean Time to Repair/Resolve (Severity 1 Items)

**Definition:** Mean Time to Repair (Severity 1 Items) will be calculated by determining time (stated in hours and minutes) representing the statistical mean for all Severity 1 Defects for in-scope deliverables in the Contract Month. “Time to Repair” is measured from time and Issue is received at the Contractor Issue/Defect tracking system to point in time when the Defect is resolved or workaround is in place and the Contractor submits the repair to the State for confirmation of resolution.

“Severity 1 Defect Service Request” means an incident where the State’s use of a solution service element has stopped or is so severely impacted that the State personnel cannot reasonably continue to work.

This Service Level begins upon Contractor presentation of a deliverable (generally code based) to the State for conducting Acceptance Testing and when this deliverable is initially migrated or otherwise used in a production environment.

**Formula:** Mean Time to Repair (Severity 1 Outages) 
$$\frac{\text{(Total elapsed time it takes to repair Severity 1 Defect Service Requests)}}{\text{(Total Severity 1 Defect Service Requests)}}$$

**Measurement Period:** Month

**Data Source:** Monthly Project Report

**Frequency of Collection:** Per Incident

#### Service Level Measures

Individual SLGYR State	Incident Resolution – Mean Time to Repair (Severity 1 Defects).
Green	<=24 hours
Yellow	>2 4 hours and <= 48 hours
Red	>48 hours

## 8.5.2. Defect Resolution – Mean Time to Repair/Resolve (Severity 2 Items)

**Specification:** Defect Resolution – Mean Time to Repair/Resolve (Severity 2 Items)

**Definition:** Mean Time to Repair (Severity 2 Items) will be calculated by determining time (stated in hours and minutes) representing the statistical mean for all Severity 2 Defects for in-scope deliverables in the Contract Month. “Time to Repair” is measured from time and Issue is received at the Contractor Issue/Defect tracking system to point in time when the Defect is resolved or workaround is in place and the Contractor submits the repair to the State for confirmation of resolution.

“Severity 2 Defect Service Request” means an incident where the State’s Software or Processing Error that results in a partial or intermittent system outage or unavailability, performance Items that result in undue delay of processing business cycle data and creation of a processing backlog, System performance and availability levels not adhering to agreed-upon SLAs, the State’s traditional performance levels, and generally accepted and customary industry standards for similar functions or capabilities, a temporary workaround identified but due to processing, hardware, labor or other considerations is deemed unreasonable by the State, or may be a recurring issue with identified or indeterminate cause.

This Service Level begins upon Contractor presentation of a deliverable (generally code based) to the State for conducting Acceptance Testing and when this deliverable is initially migrated or otherwise used in a production environment.

**Formula:** Mean Time to Repair (Severity 2 Outages) 
$$\frac{\text{(Total elapsed time it takes to repair Severity 2 Defect Service Requests)}}{\text{(Total Severity 2 Defect Service Requests)}}$$

**Measurement Period:** Accounting Month

**Data Source:** Monthly Project Report

**Frequency of Collection:** Per Incident

### Service Level Measures

Individual SL GYR State	Incident Resolution – Mean Time to Repair (Severity 2 Defects).
Green	<= 72 hours
Yellow	> 72 hours and <= 90 hours
Red	> 90 hours

### 8.5.3. Defect Resolution – Mean Time to Repair/Resolve (Severity 3 Items)

**Specification:** Defect Resolution – Mean Time to Repair/Resolve (Severity 3 Items)

**Definition:** Mean Time to Repair (Severity 3 Items) will be calculated by determining time (stated in hours and minutes) representing the statistical mean for all Severity 3 Defects for in-scope deliverables in the Contract Month. “Time to Repair” is measured from time and Issue is received at the Contractor Issue/Defect tracking system to point in time when the Defect is resolved or workaround is in place and the Contractor submits the repair to the State for confirmation of resolution.

“Severity 3 Defect Service Request” means an incident where the State’s Software or Processing Error that results in a partial or intermittent system outage or unavailability, performance items that result in periodic, but not otherwise undue delay of processing business cycle data and creation without the creation of a processing backlog that spans a business cycle, system performance and availability levels not adhering to agreed-upon performance parameters, the State’s traditional performance levels, and generally accepted and customary industry standards for similar functions or capabilities, errors or omissions in the software, related software elements, operational processes or software integration suite for which a workaround exists, but have been reported to and accepted by the Contractor, an acceptable State agreed workaround has been identified and implemented, temporary workaround identified with State acceptable processing, hardware, labor or other considerations, may be a recurring issue with identified or indeterminate cause, and items otherwise not classified as a Severity 1 or Severity 2 Defect.

This Service Level begins upon Contractor presentation of a deliverable (generally code based) to the State for conducting Acceptance Testing and when this deliverable is initially migrated or otherwise used in a production environment.

**Formula:** 
$$\frac{\text{Mean Time to Repair (Severity 3 Outages)} \times (\text{Total elapsed time it takes to repair Severity 3 Defect Service Requests})}{(\text{Total Severity 3 Defect Service Requests})}$$

**Measurement Period:** Accounting Month

**Data Source:** Monthly Project Report

**Frequency of Collection:** Per Incident

#### Service Level Measures

Individual SL GYR State	Incident Resolution – Mean Time to Repair (Severity 3 Defects).
Green	<= 7 calendar days
Yellow	> 7 calendar days and <= 10 calendar days
Red	> 10 calendar days

### 8.5.4. Service Levels – Testing Performance

**Specification:** System Test Execution Exit Quality Rate

**Definition:** System Test Execution Exit Quality Rate will be determined using the results of Contractor generated pre-test strategy, executed testing cases including functionality, performance, integration, interfaces, operational suitability and other test coverage items comprising a thorough Contractor executed system testing effort.

“System Test Execution Exit Quality Rate” means the inventory of all test cases performed in conjunction with Contractor system testing, or testing otherwise preceding the State’s User Acceptance Testing efforts, presentation of resultant test performance inclusive of identified errors or issues (by Severity), impact areas and overall testing results to the State otherwise referred to as “Testing Results”.

This Service Level begins upon Contractor presentation of the aforementioned Testing Results to the State prior to the State conducting UAT. The initial service level shown for this SLA will be 90.0%, exclusive of Severity 1 issues (which must be resolved prior to presentation to the State)and will be validated during an initial measurement period. Following the initial measurement period, and for all releases, updates, enhancements or patches and as a result of any production or commercial use the initial Service Level will be 95%. The initial measurement period will be as mutually agreed by the Parties, not to exceed three months and only pertain to the first production release.

**Formula**

$$\text{Test Quality Exit Rate} = \frac{\text{(Total \# of Test Scripts Passed during Final Pass of System Test)}}{\text{(Total \# of Test Scripts Executed during Final Pass of System Test)}} \times 100$$

**Measurement Period:** Accounting Month

**Data Source:** Monthly Project Report

**Frequency of Collection:** At end of System Test

#### Service Level Measures

Individual SL GYR State	System Testing Test Execution Exit Quality Rate
Green	>= 90%
Yellow	>= 85%, <90%
Red	< 85%

### 8.5.5. Blocking Issues – Identification and Removal

**Specification:** Testing of Blocking Issues – Identification and Removal Rate

**Definition:** A “blocking issue” is an item that is non-compliant, or otherwise fails to meet the overall quality standard agreed for work comprising a release or otherwise described in an approved statement of work between the Contractor and the State, that without remediation causes testing or production efforts to be halted, delayed or blocked for a delivery element, a logical system function or set of functions up to and including the overall work product contracted by the State.

If a blocking issue is identified, and meets the standard of prohibiting the State to reasonably conclude testing and accepting a release or SOW in part or in full, meaning no more testing (or promotion to a production environment in a reliable or timely manner) can be completed prior to resolution of the blocking issue, the Contractor will remedy the issue or deliver suitable working and commercially viable alternatives to the State as to resume testing activities and meet the business requirement as requested by the State.

This Service Level begins upon Contractor presentation of the aforementioned Testing Results to the State prior to the State conducting UAT. The initial service level shown for this SLA will be 10.0% and will be validated during an initial measurement period. Following the initial measurement period, and as a result of any production or commercial use the initial Service Level will be adjusted to 5%. The initial measurement period will be as mutually agreed by the Parties, not to exceed three months.

**Formula:**

$$\frac{\text{\% of time lost to blocking issues} \times (\text{Total Test Time Lost to Blocking Issues})}{(\text{Total Scheduled Test Time})} \times 100$$

**Measurement Period:** Accounting Month

**Data Source:** Monthly Project Report

**Frequency of Collection:** Per Incident

#### Service Level Measures

Individual SL GYR State	Blocking Issue Identification and Removal
Green	<= 10%
Yellow	>10%, <= 12%
Red	<= 15%

### 8.5.6. Regression Testing Performance – Issue Find/Fix Rate

**Specification:** Issue Find/Fix Rate

**Definition:** Regression Testing Issue find fix rate is the time the Contractor spends resolving issues identified during UAT testing as a percentage of the time required to develop the code content associated with a release, enhancement, maintenance fix or otherwise identified for production execution.

The State would like to ensure the Contractor has a prompt response to addressing issues detected during testing and ensure that the Contractor is well aligned with removal of issues detected during testing efforts and that there is a prompt return of the fix to be included in the regression testing process.

This Service Level begins upon Contractor presentation of the aforementioned Testing Results to the State prior to the State conducting UAT. The initial service level shown for this SLA will be 10.0% and will be validated during an initial measurement period. Following the initial measurement period, and as a result of any production or commercial use the initial Service Level will be adjusted to 5%. The initial measurement period will be as mutually agreed by the Parties, not to exceed three months.

“Time spent in Regression Fix” is the development time required for fixing UAT defects which cause UAT testing to stop or be delayed past the scheduled test completion date. The sum of this time is then rounded (using standard rounding) to result in the number of days.

“Time spent in Regression Test” is measured as the number of days that are added to the original UAT Test schedule due to test defect or issue resolution and additional testing having to occur due to regression testing of identified UAT defects.

“Total Development Time for Release in Days” is measured as the total time for the Release prior to the UAT phase for development and systems testing activities performed by the Contractor.

Should issues be identified and resolved within the planned UAT period, this SLA will not apply.

**Formula:**

$$\frac{\text{\% of Time Repairing Issues} \times (\text{Time spent in Regression Fix} + \text{Time Spent in Regression Test (Days)})}{(\text{Total Development Time for Release in Days})} \times 100$$

**Measurement Period:** Accounting Month

**Data Source:** Monthly Project Report

**Frequency of Collection:** At end of UAT phase for each release to Production

#### Service Level Measures

Individual SLGYR State	Issue Find/Fix Rate
Green	<= 10%
Yellow	>10%, <= 12%
Red	<= 15%

### 8.5.7. Code Coverage – Automated Test Beds

**Specification:** % Automated Code Coverage – Regression, Release and Performance Testing

**Definition:** Amount of Code that is covered using automated testing tools for performance, functionality or scenario testing pertaining to (re)testing items or releases that had been previously tested under prior releases OR performance testing of the system or release element and relationships between a release item and its relationships to production code.

The Contractor is to provide best practices in conjunction with the overall testing effort. To facilitate rapid and quality testing, with a high degree of code coverage, the Contractor will employ automated testing tools and techniques where possible to test core scenarios, scenario variations, regression testing and performance testing

This SL will commence upon the delivery of a function set to the Contractor System testing environment and be in effect during the overall testing effort including Contractor efforts, joint efforts or in support of the State activities as agreed and apply to initial testing elements, regression/fix elements, performance and integration testing prior to production use.

**Formula:**

$$\frac{\text{Number of Test Cases covered by Automated Testing Tool within a Testing Period} + \text{Total Number of Performance Test Cases covered by Automated Performance Test Tool}}{\text{Number of total Test Cases within a Testing Period} + \text{Total Number of Performance Test Cases within a Testing Period}} \times 100$$

% of Code covered by Automated tools

**Measurement Period:** Weekly, During Testing

**Data Source:** Weekly Project Report

**Frequency of Collection:** Mutually Agreed Testing Periods

#### Service Level Measures

Individual SL GYR State	% Automated Code Coverage
Green	>75%
Yellow	>50%, <= 75%
Red	<= 50%

### 8.5.8. Service Levels – Project Performance

**Specification:** % Compliance Milestone Dates

**Definition:** Amount of committed and accepted Project Milestones achieved on time as per the Project plans.

The Contractor is to produce an overall Project plan inclusive of the milestones, activities and deliverables at the commencement of the Project. Due to the overlapping nature of phases, tasks and activities, a measurement period of 1 calendar month will be established to serve as the basis for the measurement window. Vendor will count all milestones, activities and deliverables to be completed during that measurement window and their corresponding committed delivery dates. Any date variations (positive or negative) will be recorded upon the State’s acceptance of the deliverable and used in the calculation of this SL.

This SL will commence upon Project initiation and will prevail until Project completion.

**Formula:** 
$$\frac{\text{Total Number of Contractor Milestones met within the measurement month}}{\text{Total Number of Contractor Milestones planned to be met during the measurement month per the agreed upon list of milestones}} \times 100$$

% Compliance, Milestone Dates

**Measurement Period:** Monthly, During Project

**Data Source:** Weekly Project Report

**Frequency of Collection:** Weekly

#### Service Level Measures

Individual SL GYR State	% Compliance Milestone Dates
Green	> 90%
Yellow	>85%, <=90%
Red	<= 85%

### 8.5.9. Issue Reporting

**Specification:** % Compliance Issue Reporting

**Definition:** The reporting of any issues impacting the Project to the State for prompt resolution and possible solutions to the State. The Contractor is to promptly report all issues to the Project management and sponsorship personnel within the State upon detection of an issue that will impact overall Project delivery, Project quality, or overall effectiveness of the Project in its intended production operation mode.

Wherever possible, the Contractor must include recommendations as to work-arounds, remedial actions, impact assessment and potential mitigation strategies the State may employ.

This SL will commence upon Project initiation and will prevail until Project completion.

**Formula:**

$$\begin{aligned}
 \text{\% Compliance, Issue Reporting} &= \frac{\text{\# Project Issues Identified during reporting period} - \text{Issues not reported during period Status Reports} - \text{\# issues - Other unreported Issues that arise or are discovered subsequent to reporting dates}}{\text{\# Project Issues Identified during reporting period}} \times 100
 \end{aligned}$$

**Measurement Period:** Monthly, During Project

**Data Source:** Weekly Project Report

**Frequency of Collection:** Weekly

Individual SL GYR State	% Compliance Issue Reporting
Green	>90%
Yellow	>85%, <=90%
Red	<= 85%

## 8.5.10. Deliverable Acceptance

**Specification:** % Deliverable Acceptance

**Definition:** The State’s ability to accept Contractor deliverables based on submitted quality and in keeping with initially defined standards and content for Contractor deliverables.

The Contractor must provide deliverables to the State in keeping with agreed levels of completeness, content quality, content topic coverage and otherwise achieve the agreed purpose of the deliverable between the State and the Contractor. For the avoidance of doubt, the deliverables contained in this RFP as they pertain to the Shared Services Implementation Project and general Ongoing Project Services delivery concepts associated with structured software development will represent the minimum set of expected deliverables.

Notwithstanding the State review and approval cycles, this SL will commence upon the delivery of a final deliverable for acceptance to the State, and any work/re-work to the final deliverable as a result of any State questions, required clarifications/amplifications, and conclude upon due completion of the required amendments.

This SL will commence upon Project initiation and will prevail until Project completion.

**Formula:**

$$\frac{\text{\% Deliverable Acceptance} \times \text{\# Deliverables Accepted During Period (less the State review Time)}}{\text{\# Deliverables Presented during Period}} \times 100$$

**Measurement Period:** Monthly, During Project

**Data Source:** Weekly Project Report

**Frequency of Collection:** Weekly

### Service Level Measures

Individual SL GYR State	% Deliverable Acceptance
Green	>85%
Yellow	>80%, <=85%
Red	<= 80%

### 8.5.11. Support of State User Acceptance Testing Activities

**Specification:** Support of the State User Acceptance Testing (UAT) activities

**Definition:** The Contractor must support the State UAT activities based on their knowledge of the overall system, responsibility to maintain environments, regression test beds, automated tools and retained developers on the Project to affect prompt and quality resolutions to issues detected by the State during a UAT phase.

Testing environments are to be functional and available to the State to conduct UAT activities, configured with all required base configuration and test data, application code and other elements as required to support the overall State testing effort.

The Contractor must provide a system(s) to accept and track any issues, defects or questions arising from the State during the performance of UAT functions, and acknowledge all issues with an estimate to resolve these issues within 2 business hours of receipt of the issue.

This SL will commence upon the delivery of a function set to the State to perform any User Acceptance or Validation and be in effect during the overall State testing effort including Contractor efforts, joint efforts or in support of the State activities as agreed and apply to initial testing elements, regression/fix elements, performance and integration testing prior to production use.

NOTE: All issues, defects, or questions will be recorded in a mutually agreeable tool and will be acknowledged with an estimate to resolve within 2 business hours.

**Formula:**

$$\begin{aligned}
 & \# \text{ Business Hours, Seven Days Per Week During UAT Period} \\
 & - (\text{minus}) \\
 & \% \text{ UAT Support} = \frac{(\# \text{ hours testing environments unavailable or unusable to perform testing} + \text{number business hours beyond standard State inquiries are not acknowledged and estimated})}{\# \text{ Business Hours, Seven Days Per Week During UAT Period}} \times 100
 \end{aligned}$$

**Measurement Period:** Monthly, During Project

**Data Source:** Weekly Project Report

**Frequency of Collection:** Monthly

#### Service Level Measures

Individual SL GYR State	% UAT Support
Green	>85%
Yellow	>80%, <=85%
Red	<= 80%

## 8.5.12. Service Levels – Development Methodology Compliance

**Specification:** %SDLC Compliance.

**Definition:** The Contractor will present and adapt as required a Software Development Lifecycle (SDLC) Methodology to manage the end-to-end software delivery process. This process will be followed.

The Contractor must provide as part of overall Project delivery a proven and tested SDLC to drive and govern the overall software development process and adapt wherever possible to accommodate State considerations and processes. Based on this SDLC and the prescribed development stages (e.g., requirements, design, build, test, deployment) and phase exit documentation, reviews and signoff, this process will be followed for the duration of all development or code based Projects contracted by the State.

Notwithstanding State review and approval cycles, this SL will commence upon Project initiation and will prevail until Project completion.

**Formula:**

$$\% \text{ SDLC Compliance} = \frac{\# \text{ Deliverables, Milestones, Activities, Reviews and Signoffs Missed Per Phase/SDLC Gate}}{\# \text{ Deliverables, Milestones, Activities, Reviews and Signoffs Required Per Phase/SDLC Gate}} \times 100$$

**Measurement Period:** Monthly, During Project

**Data Source:** Weekly Project Report

**Frequency of Collection:** Weekly

### Service Level Measures

Individual SL GYR State	% SDLC Compliance
Green	>95%
Yellow	>90%, <=95%
Red	<= 90%

### 8.5.13. Service Levels–Project Delivery–Build/Test Activities as a Percentage of Overall Activities

**Specification:** % build and testing activities

**Definition:** The Contractor will perform (subject to other SLAs in effect) and prioritize deliverable construction efforts in keeping with overall Project plans and focus effort on deliverable creation and completion associated with the successful delivery of a working Project delivered with quality to a production environment.

The Contractor must report the overall date and quality considerations of the Project delivery for the SOW governing this SL, the amount of time doing constructive efforts in building software elements, deliverables, and associated documentation; and conducting testing (system, integration, interface and performance) as a percentage of overall activities during the measurement period.

This SL will commence upon Project initiation and will prevail until Project completion.

Prior to the Start of the Build and Test Phases, the State and Contractor will forecast the number of development objects and test scripts in a schedule (**planned** number submitted by month) for the phase. Each Team Lead will track the **actual** number of completed development objects and test scripts and report progress during status meetings with project leadership.

**Formula:** % Time Spent in Build and Testing Activities Actual Number of Work Units Submitted in a Month (cumulative for phase or release)

$$\frac{\text{Actual Number of Work Units Submitted in a Month}}{100\% \text{ Planned Number to be Submitted at Month End (cumulative for phase or release)}} \times 100$$

% Estimating Accuracy

**Measurement Period:** Monthly, During Project

**Data Source:** Weekly Project Report

**Frequency of Collection:** Weekly

#### Service Level Measures

Individual SL GYR State	% Build and Testing Activities
Green	>75%
Yellow	>70%, <=75%
Red	<= 70%

### 8.5.14. Service Levels – Project Completion – Issues Detected and Resolved In Production

**Specification:** Issues Detected and Resolved in Production

**Definition:** During post-implementation the Contractor must continue to support and promptly resolve any issues emerging as a result of the implementation in a production environment for a period of 45 days or otherwise mutually agreed upon, or until such time as a Managed Services SL is in effect for the element in question.

The Contractor must measure all production exceptions, issues, or problems associated or in conjunction with the initial 45 day period associated with a move of a software release to a production environment regardless of the severity level unless otherwise agreed with the State. Function points from system and user acceptance testing will serve as the basis for counting the total number of elements associated with a release.

This SL will commence upon promotion of code associated with the Project to a production or commercial environment and will prevail until all issues are resolved to the State’s satisfaction or 45 days, whichever is longer.

**Formula:**

$$\frac{\text{Issues Identified and Resolved in Production}}{\text{Total Hours included in a Production Release}} \times 100$$

Total Time Required to Resolve Issues Identified During initial 90 day production Period

**Measurement Period:** Monthly, During Project

**Data Source:** Weekly Project Report

**Frequency of Collection:** Weekly

#### Service Level Measures

Individual SL GYR State	Issues Detected and Resolved in Production
Green	<= 2%
Yellow	>2%, <=3%
Red	>3%

## 9.0 Service Level Requirements: State BI / Data Warehouse Operations / Run

This section sets forth the performance specifications for the Service Level Agreements (SLA) and Service Level Objectives (SLO) to be established between the Contractor and the State that are applicable to any work associated with the operation, maintenance, updates or upgrades of any software associated with this Supplement in general, and under Section 2 specifically as the work pertains to any BI Operations and Run services.

The section contains the tables and descriptions that provide the State framework, requirements relating to service level commitments, and the implications of meeting versus failing to meet the requirements and objectives, as applicable. This document defines the State's detailed performance, management, and reporting requirements for the Operations and Run Services and to all subsequent Operations and Run services and phases that are contracted under future Statements of Work between the State and the Contractor related to this RFP.

The mechanism set out herein will be implemented to manage the Contractor's performance against each Service Level, in order to monitor the overall performance of the Contractor.

The Contractor will be required to comply with the following performance management and reporting mechanisms for all Services within the scope of this RFP and will provide these reports to the State on a no less frequent than monthly basis:

- **Service Level Specific Performance** – Agreed upon specific Service Levels to measure the performance of specific Services or Service Elements. Most individual Service Levels are linked to financial credits due to the State ("Performance Credits") to incent Contractor performance.
- **Overall Contract Performance** – An overall performance score of the Contractor across all Service Levels. The overall performance score is linked to governance and escalation processes as-needed to initiate corrective actions and remedial processes.

### 9.1. Service Level Specific Performance Credits

Each Service Level (SL) will be measured using a "Green-Yellow-Red" traffic light mechanism (the "Individual SL GYR State"), with "Green" representing the highest level of performance and "Red" representing the lowest level of performance. A Performance Credit will be due to the State in the event a specific Individual SLA GYR State falls in the "Yellow" or "Red" state. The amount of the Performance Credit for each SLA will be based on the Individual SLA GYR State. Further, the amounts of the Performance Credits will, in certain cases, increase where they are imposed in consecutive months. No Service Level Performance Credit will be payable for the Contractor's failure to meet a Service Level Objective.

Set forth below is a table summarizing the monthly Performance Credits for each SLA. All amounts set forth below that are contained in a row pertaining to the "Yellow" or "Red" GYR State, represent Performance Credit amounts.

Consecutive (SLA Performance Credits)												
Individual SL GYR State	1st Month	2nd Month	3rd Month	4th Month	5th Month	6th Month	7th Month	8th Month	9th Month	10th Month	11th Month	12th Month
Red	A =1.71% of MPC	A + 50% of A	A + 100% of A	A + 150% of A	A + 200% of A	A + 250% of A	A + 300% of A	A + 350% of A	A + 400% of A	A + 450% of A	A + 500% of A	A + 550% of A
Yellow	B = 0.855% of MPC	B + 50% of B	B + 100% of B	B + 150% of B	B + 200% of B	B + 250% of B	B + 300% of B	B + 350% of B	B + 400% of B	B + 450% of B	B + 500% of B	B + 550% of B
Green	None	None	None	None	None	None	None	None	None	None	None	None

The Contractor agrees that in each month of the Contract, 12% of the monthly project charges (MPC) associated with the Project Implementation portion of this RFP will be at risk. MPCs are the charges for the deliverables accepted during a given month. The MPC for the Project Implementation will be at risk for failure to meet the Service Levels set forth in the Contract. The Contractor will not be required to provide Performance Credits for multiple Performance Specifications for the same event; the highest Performance Credit available to the State for that particular event will apply.

On a quarterly basis, there will be a “true-up” at which time the total amount of the Performance Credits will be calculated (the “Net Amount”), and such Net Amount will be set off against any fees owed by the State to the Contractor.

Moreover, in the event of consecutive failures to meet the Service Levels, the Contractor will be required to credit the State the maximum Performance Credit under the terms of the Contract.

The Contractor will not be liable for any failed Service Level caused by circumstances beyond its control, and that could not be avoided or mitigated through the exercise of prudence and ordinary care, provided that the Contractor immediately notifies the State in writing and takes all steps necessary to minimize the effect of such circumstances and resumes its performance of the Services in accordance with the SLAs as soon as possible.

For example, if an Individual SL GYR State is Yellow in the first Measurement Period, Red in the second Measurement Period and back to Yellow in the third Measurement Period for an SLA then the Performance Credit due to the State will be the sum of Yellow Month 1 (B) for the first Measurement Period, Red Month 2 (A + 50% of A) for the second Measurement period, and Yellow Month 3 (B + 100% of B) for the third Measurement period, provided (1) such Performance Credit does not exceed 12% of the MPC (the At-Risk Amount); and, (2) no single Service Level Credit will exceed 20% of the total At-Risk Amount, as stated below:

SLA Calculation EXAMPLE						
Monthly Project Charge (MPC) = \$290,000.00						
Monthly At Risk Amount = 12% of MPC = \$34,800						
Maximum for any one SLA = 20% of At Risk Amount = \$6,960						
GYR State	1 <sup>st</sup> Month		2 <sup>nd</sup> Month		3 <sup>rd</sup> Month	
Red	0	\$	0	\$7,438.50	0	
Yellow	1	\$2,479.50	1		1	\$4,959.00
Green	6	\$	6		6	
Totals	7	\$2,479.50	7	\$7,438.50	7	\$4,959.00
Adjusted Totals by At Risk Amount and 20% per individual SLA Limitations	(Is monthly total of all Service Level Credits equal to or less than \$34,800?) - Yes (Is monthly amount for any one Service Level Credit equal to or less than \$ 6,960?) - Yes \$2,479.50		(Is monthly total of all Service Level Credits equal to or less than \$34,800?) - Yes (Is monthly amount for any one Service Level Credit equal to or less than \$ 6,960?) - No \$6,960.00		(Is monthly total of all Service Level Credits equal to or less than \$34,800?) - Yes (Is monthly amount for any one Service Level Credit equal to or less than \$ 6,960?) - Yes \$4,959.00	
Total Quarterly Credit:	\$ 2,479.50 +		\$ 6,960.00 +		\$ 4,959.00	
Total Quarterly Credit: \$ 14,398.50						

Service Level Performance Credit payable to the State = (B) + (A + 50% A) + (B + 100% B), based on an illustrative MPC of \$290,000;

The total of any weighting factors may not exceed 100% of the total At-Risk Amount. To further clarify, the Performance Credits available to the State will not constitute the State’s exclusive remedy to resolving issues related to the Contractor’s performance. Service Levels will commence with Project initiation for any Implementation Project.

## 9.2. Overall Contract Performance

In addition to the service specific performance credits, on a monthly basis, an overall SL score (the “Overall SL Score”) will be determined, by assigning points to each SL based on its Individual SL GYR State. The matrix set forth below describes the methodology for computing the Overall SL Score:

Individual SLAs and SLOs GYR State	Performance Multiple
Green	0
Yellow	1
Red	4

The Overall SL score is calculated by multiplying the number of SLAs and SLOs in each GYR State by the Performance Multiples above. For example, if all SLAs and SLOs are Green except for two SLAs in a Red GYR State, the Overall SL Score would be the equivalent of 8 (4 x 2 Red SLAs).

Based on the Overall SL Score thresholds value exceeding a threshold of fifteen (15), mandatory Executive escalation procedures outlined in this RFP will be initiated to restore acceptable Service Levels.

If a successful resolution is not reached, then **the State may terminate the Contract for cause if:**

The overall SL score reaches a threshold over a period of 3 consecutive months with the equivalent of 50% of the service levels in a red state; and the Contractor fails to cure the affected Service Levels within 60 calendar days of receipt of the State’s written notice of intent to terminate; **OR**

The State exercises its right to terminate for exceeding the threshold level of 75% of Service levels in total over a six (6) month period.

**The Overall Contract Performance will not constitute the State’s exclusive remedy to resolving issues related to the Contractor’s performance. The State retains the right to terminate for Overall Contract Performance under the terms of this Contract.**

### 9.3. Monthly Service Level Report

On a State accounting monthly basis, the Contractor will provide a written report (the “Monthly Service Level Report”) to the State which includes the following information: (i) the Contractor’s quantitative performance for each Service Level; (ii) each Individual SL GYR State and the Overall SL Score; (iii) the amount of any monthly Performance Credit for each Service Level (iv) the year-to-date total Performance Credit balance for each Service Level and all the Service Levels; (v) a “Root-Cause Analysis” and corrective action plan with respect to any Service Levels where the Individual SL GYR State was not “Green” during the preceding month; and (vi) trend or statistical analysis with respect to each Service Level as requested by the State . The Monthly Service Level Report will be due no later than the tenth (10th) accounting day of the following month.

**Failure to report any SLA, SLA performance in a given month, or for any non-Green (i.e., performing to Standard) SLA a detailed root cause analysis that substantiates cause will result in the State considering the performance of the Contractor for that period as performing in a Red State.**

### 9.4. Failure to Report or Report Late after Mutually Agreed Dates

Should for any reason the Contractor fail to report or produce the Monthly Service Level Report to the State on a mutually agreeable date, in part or in total, the Contractor performance for the Service Levels, in part or in total, shall be considered Red for that period. Should, under agreement of the State a Service Level not apply in a given period, the report shall reflect this agreement and indicate “not applicable this period”.

### 9.5. BI Applications and Environments

The State acknowledges that its BI environment requirements fall into two major categories: 1) critical applications – those that are required to perform day-to-day state functions in production or support the SDLC requirements for major infrastructure investments for major initiatives where significant funds are devoted to providing environments to development teams; and 2) non-critical application environments – which are defined as items that do not have a significant impact on day-to day operations, are used in a non-production capacity, which may not adversely impact the productivity of State development efforts or are otherwise used to support non-commercial activities. The Contractor must deliver Service Levels in keeping with the criticality levels as described herein.

### 9.6. Period Service Level in Full Effect and In-Progress Service Levels

Service levels specified herein shall be in full effect no later than ninety (90) days following the completion of migration of the current services and environments to the Contractor’s responsibility. During the phases in which the Contractor is performing Transition/Migration Services and while the State and the existing MSV still retain operational responsibility of the application environments, the Contractor will not be subject to financial credits associated with the Service levels described herein, but nonetheless shall be required to report the service levels as specified. During the period in which the State and existing MSV no longer have substantive operational responsibilities pertaining to the application environments, and the Contractor is operating application environments for the State, or a combination of State and Contractor responsibilities the Contractor agrees to:

- a) Perform services in keeping with the described Service Levels contained herein;

- b) Promptly report any Service Level violations in accordance with the Service Level reporting requirements contained herein;
- c) Work in good faith and using commercially reasonable efforts to address and otherwise resolve service level violations that arise;
- d) Provide a level of service in keeping with levels performed by State personnel and otherwise aligned with commercial best practices prior to the operational transfer; and
- e) Not be subject to any financial credits associated with Service Level violations.

Due to the nature of the implementation of future Major Projects or new modules associated with OAKS, full SLAs will not be in effect for the applications until such time as either module is moved to a production environment or is used for commercial use, whichever is sooner. During a period of ninety (90) calendar days immediately following a production migration or commercial use, or an alternative period otherwise agreed by the State, the acceptable performance during this stabilization period shall be no less than a “yellow” status and financial credits shall not apply unless the Major Project or module is deemed to be performing in a RED state.

### 9.7. Temporary Escalation of an SLO to an SLA

In general, SLOs are considered measurable objectives by the State and the SLA framework accommodates their treatment and importance to the State via Contract termination considerations as opposed to financial credits as contained herein. However, in the event that Contractor performance is not meeting the established standards and requirements for SLO related items, the State may determine that an SLO needs to be escalated to an SLA. The following conditions shall prevail in this escalation:

- Contractor performance falls below yellow standard in an SLO area for three consecutive months; or
- Contractor performance falls below 75% of red standard in any given month; or
- Contractor performance is consistently in a yellow or red status for four of any six consecutive months.

Should one or more of these conditions exist, the State may:

- Temporarily replace any SLA of it's choosing with the SLO until such time as the below standard SLO is determined to be consistently (i.e., more than 3 months in a row) performing to standard;
- Add the SLO to the SLA group and rebalance the weighting accordingly such that the monthly fees at risk percentage agreed to is maintained (i.e., fees at risk remain constant, the number of SLAs that are considered against those fees changes) until such time as the below standard SLO is determined to be consistently (i.e., more than 3 months in a row) performing to standard.

At the conclusion of period of three consecutive months where the escalated SLO is deemed to be performing in a green status, the State and Contractor will revert the escalated SLO (now an SLA) back to its SLO state.

### 9.8. State Provided Service Support Infrastructure Elements

The following items not be considered Contractor Fault with respect to Service level failures and therefore not apply to any Contractor Performance Credits or Overall Contract Performance considerations discussed later in this section:

- Failures outside of the scope of the Contractor responsibilities pursuant to the Services responsibility scope;
- Failures due to non-performance of State retained responsibilities pursuant to the services responsibility scope;
- Failure of an out-of-scope State provided element that directly impacts an in-scope Contractor element;

- Failures arising from State provided equipment or networks;
- A pre-existing or undocumented deficiency in a State provided computing element as they pertain to adhering to State Policies and Standards. In this case, upon identification the Contractor is to promptly notify the State of the identified deficiency.
- Failure of a State provided resource to follow and comply with Contractor provided processes and procedures except where: (i) State Policies and Contractor policies are in conflict in which case the State resource shall notify the Contractor of the conflict and resolve which process applies or; (ii) in cases of emergency that would place the State resource at physical peril or harm;
- Failure of a State provided third party warranty or maintenance agreement to deliver services to the Contractor for in-scope services and infrastructure elements that result in the Contractor's inability to perform at required levels;
- The period of time associated with an incident where a State provided or contracted 3<sup>rd</sup> party service, repair or replacement service renders an in-scope infrastructure element unusable by the Contractor to provide the Contracted Services shall be reduced from the overall duration timing of an incident;
- The incident requires assistance for a State retained responsibility, is delayed at the State's request, or requires availability of an End User that is not available;
- Mutually agreed upon service interruptions such as scheduled changes to the technical environment.
- State implemented changes to Production Environments that the Contractor is not aware or apprised of.

## 9.9. Managed Service: Service Level Commitments

Contractor will meet the Service Level Commitment for each Service Level set forth in the table below and specified in detail later in this section

	Service Level	SLA or SLO	Coverage
1	<b>Incident Resolution – Mean Time to Repair (Severity 1 Outages)</b>	<b>SLA</b>	7x24
2	<b>Incident Resolution – Mean Time to Repair (Severity 2 Outages)</b>	<b>SLA</b>	7x24
3	Incident Resolution – Mean Time to Repair (Severity 3 Outages)	SLO	Business Hours
4	<b>Service Availability – Application Availability</b>	<b>SLA</b>	7x24
5	<b>System Performance &amp; Responsiveness</b>	<b>SLA</b>	7x24
6	Incident Resolution - Issue Triage, Closure and Recidivist Rate	SLO	Business Hours
7	User Interaction - Completion of Administrative, Root, DBA, Privileged User Adds/Deletes	SLO	Business Hours (non-emergency)
8	Security – Security Compliance	SLO	continuous
9	<b>Monitoring &amp; Auditing – Application Security Breach Detection, Notification and Resolution</b>	<b>SLA</b>	7x24
10	<b>Job Schedule and Scheduled Reporting Performance</b>	<b>SLA</b>	Scheduled Hours
11	Operational Process Control & Repeatability – Changes to Production environments	SLO	Scheduled Maintenance
12	<b>Service Quality – System Changes</b>	<b>SLA</b>	Scheduled Maintenance
13	<b>Service Timeliness – System Changes</b>	<b>SLA</b>	Scheduled Maintenance
14	<b>Data Accuracy</b>	<b>SLA</b>	continuous

Offerors are to note that for Major Projects (generally those in excess of 1,000 hours of Contractor effort) that Project level Service Level Commitments shall apply as specified in Supplement 2 which are only applicable to those Project fees or charges associated with the performance of those projects under a State Authorized Statement of Work or Change Request.

### 9.9.1. Incident Resolution – Mean Time to Repair (Severity 1 Outages)

**Business Intent:** Prompt resolution of BI outages that impact State processing and processes

**Definition:** Mean Time to Repair (Severity 1 Outages) will be determined by determining the elapsed time (stated in hours and minutes) representing the statistical mean for all Severity 1 Outage Service Requests for in-scope Services in the Contract Month. "Time to Repair" is measured from time Service Request is received at the Level 2 Service Desk to point in time when the incident is resolved or workaround is in place and the Contractor submits the resolved Service Request to the State for confirmation of resolution.

"Severity 1 Outage" is defined as :

An Incident shall be categorized as a "Severity 1 Outage" if the Incident is characterized by the following attributes: the Incident (a) renders a business critical System, Service, Software, Equipment or network component un-Available, substantially un-Available or seriously impacts normal business operations, in each case prohibiting the execution of productive work, and (b) affects either (i) a group or groups of people, or (ii) a single individual performing a critical business function.

This Service Level begins upon completion of agreed production acceptance criteria and a measurement period as documented in the transition to production plan.

The Contractor will report updates and progress to the State every thirty (30) minutes for this SLA until resolved.

**Formula:**

$$\text{Mean Time to Repair (Severity 1 Outages)} = \frac{\text{Total elapsed time it takes to repair Severity 1 Outage Service Requests}}{\text{Total Severity 1 Outage Service Requests}}$$

**Measurement Period:** Reporting Month

**Data Source:** Monthly Service Report

**Frequency of Collection:** Per incident

**Service Level Measures:**

Individual SL GYR State	Mean Time to Repair (Severity 1 Outages).
Green	<= 4 hours
Yellow	> 4 hours and <= 6 hours
Red	> 6 hours

## 9.9.2. Incident Resolution – Mean Time to Repair (Severity 2 Outages)

**Business Intent:** Prompt resolution of BI outages that impact State processing and processes

**Definition:** Mean Time to Repair (Severity 2 Outages) will be determined by determining the elapsed time (stated in hours and minutes) representing the statistical mean for all Severity 2 Outage Service Requests for in-scope Services in the Contract Month. "Time to Repair" is measured from time Service Request is received at the Level 2 Service Desk to point in time when the incident is resolved or workaround is in place and the Contractor submits the resolved Service Request to the State for confirmation of resolution.

"Severity 2 Outage" is defined as : An Incident shall be categorized as a "Severity 2 Outage" if the Incident is characterized by the following attributes: the Incident (a) does not render a business critical System, Service, Software, Equipment or network component un-Available or substantially un-Available, but a function or functions are not Available, substantially Available or functioning as they should, in each case prohibiting the execution of productive work, and (b) affects either (i) a group or groups of people, or (ii) a single individual performing a critical business function.

This Service Level begins upon completion of agreed production acceptance criteria and a measurement period as documented in the transition to production plan.

In the event of "go live" of new functionality, an Upgrade, or significant change in the architecture of the Application environment, this Service Level will be suspended temporarily from the time the "go live" of the applicable Change through two (2) business days following completion of stabilization criteria in accordance with the transition to production plan.

The Contractor will report updates and progress to the State every sixty (60) minutes for this SLA until resolved.

**Formula:**

$$\text{Mean Time to Repair (Severity 2 Outages)} = \frac{\text{Total elapsed time it takes to repair Severity 2 Outage Service Requests}}{\text{Total Severity 2 Outage Service Requests}}$$

**Measurement Period:** Reporting Month

**Data Source:** Monthly Service Report

**Frequency of Collection:** Per incident

### Service Level Measures:

Individual SL GYR State	Mean Time to Repair (Severity 2 Outages).
Green	<= 8 hours
Yellow	> 8 hours and <= 12 hours
Red	> 12 hours

### 9.9.3. Incident Resolution – Mean Time to Repair (Severity 3 Outages)

**Business Intent:** Prompt resolution of BI issues and irregularities that impact State processing and processes

**Definition:** Mean Time to Repair (Severity 3 Outages) will be determined by determining the elapsed time (stated in hours and minutes) representing the statistical mean for all Severity 3 Outage Service Requests in the Contract Month.

“Time to Repair” is measured from time a Service Request for in-scope Services is received at the Level 2/3 Contractor Service Desk to point in time when the incident is resolved or workaround is in place and the Contractor submits the resolved Service Request to the State for confirmation of resolution.

“Severity 3 Outage” Is defined as :

An Incident shall be categorized as a “Severity 3 Outage” if the Incident is characterized by the following attributes: the Incident causes a group or individual to experience a Incident with accessing or using a System, Service, Software, Equipment or network component or a key feature thereof and a reasonable workaround is not available, but does not prohibit the execution of productive work.

This Service Level begins upon completion of agreed production acceptance criteria and a measurement period as documented in the stabilization and transition to production plan.

The Contractor will report updates and progress to the State every twenty-four (24) hours for this SLA until resolved.

**Formula:**

$$\text{Mean Time to Repair (Severity 3 Outages)} = \frac{\text{(Total elapsed time it takes to repair Severity 3 Outage Service Requests)}}{\text{Total Severity 3 Outage Service Requests}}$$

**Measurement Period:** Reporting Month

**Data Source:** Monthly Service Report

**Frequency of Collection:** Per incident

**Service Level Measures:**

Individual SL GYR State	Mean Time to Repair (Severity 3 Outages).
Green	<= 5 business days
Yellow	> 5 business days <=7 business days
Red	> 7 business days

## 9.9.4. Service Availability – Application Availability

**Business Intent:** BI is Available to All State Users for All Business Functions to Support Critical State Financial, HR and Procurement Processes.

**Definition:** Application Availability for each in-scope Platform, Environment, Module and Business Process

Application Availability means access to the production system is enabled; log-in permitted from the local user LAN and business transactions can be executed. While it is dependent on State provided infrastructure and Third Party software availability the expectation is that the Contractor will implement operational processes, instrumentation, monitoring and controls that validate availability of BI to the end-user and development community in the State.

This SLA will be calculated for those Service Elements that are directly in the Contractor’s scope and will be measured from the end-user community desktop to the ability to process transactions to the BI databases. If, in determination of the root cause of an “unavailable” condition, the State LAN, WAN and Data Center outages, or the outage of State provided Infrastructure is the cause of the condition, the Contractor shall be excused from those outages that arise from such a condition, unless the outage is a direct result of a Contractor created situation.

Critical Environments shall be those that are hosting or supporting State SDLC environments for those projects in excess of \$5M in a given 12 month period and Production environments

Non-Critical Environments include routine development, testing, training, demo and the like

**Formula:**

$$\text{Application Availability} = \frac{\text{Total Application Scheduled Uptime} - \text{Total Application Unscheduled Outages}}{\text{Total Application Scheduled Uptime}}$$

**Measurement Period:** Reporting Month

**Data Source:** Monthly Service Report

**Frequency of Collection:** Continuous, 24 hours a day

**Service Level Measures:**

Individual SL GYR State	Critical/Production Environment	Non Critical Environments
<b>Green</b>	>= 99.9%	>= 99.0
<b>Yellow</b>	>= 99.7% and < 99.9%	>=95.0 and < 99.0
<b>Red</b>	<99.7%	<95.0%

### 9.9.5. System Performance and Responsiveness

**Business Intent:** BI Online and Batch Processes perform within expected norms, the end user experience is high performance and responsive and scheduled jobs, processes and reports execute within the established job schedule without intruding upon online application users or other business functions

**Definition:** System Performance and Responsiveness will be based upon an end-to-end service class performance baseline (e.g., network time, application/session response time, system time, and network return time) performed by the Contractor during the transition or as mutually agreed will perform for key service elements for a statistically valid sample of 5 EPM/BI scheduled reports.

Should the Contractor wish to accept State written requirements for each of the above in lieu of benchmarking, or use the aforementioned benchmarking, this sample shall serve as the "Performance Baseline" for this SLA.

Thereafter, the Contractor will perform automated testing on a daily basis for online transaction elements or provide objective evidence from system generated statistics, and provide run-time statistics for scheduled/batch system jobs and scheduled report and compare these to the Performance Baseline.

Two % deviations from the Performance Baseline will be calculated: 1) % Variation Online Transactions and 2) % Variation Batch/Scheduled Operations; The higher variation (i.e., online or batch) shall be used in the below formula for both the numerator and denominator

**Formula:** System Performance and Responsiveness = 
$$\frac{\text{Observed (Online or Batch Scheduled) Performance}}{\text{Baseline (Online or Batch) Performance}}$$

**Measurement Period:** Reporting Month

**Data Source:** Monthly Service Report

**Frequency of Collection:** Continuous, 24 hours a day and Schedule Job/Report Performance

**Service Level Measures:**

Individual SL GYR State	System Performance and Responsiveness
Green	< = 100%
Yellow	>100% - <=110%
Red	> 110%

### 9.9.6. Incident Resolution - Issue Triage, Closure and Recidivist Rate

**Business Intent:** Incidents affecting BI, online batch or otherwise, are promptly addressed, prioritized and resolved to the satisfaction of the State and to no reoccur or cause corollary or spurious issues to occur as a result of the repair to the element that was the root cause of the Incident.

**Definition:** Incident Triage, Closure and Recidivist Rate will be determined by monitoring compliance with the following four key performance indicators (KPI):

1. Incident Triage: Contractor to indicate high-level diagnosis and estimate to remedy to the State within 30 minutes of acknowledgement
2. Incident Closure: Incident to be documented with root cause remedy, (where root cause is within Contractor's control), and procedures to eliminate repeat of incident within 24 hours of incident close
3. Incident Recidivist Rate: Closed incidents not to reappear across all in scope Services no more than 1 times following incident closure.
4. Incident means any Severity 1 or 2 incident where the Services for which Contractor is responsible are unavailable.

**Formula:**

$$\text{Issue Triage, Closure and Recidivist Rate} = \frac{\text{Total Severity 1 and 2 Incidents for which Contractor is responsible under the SOW, where solution Services are unavailable) - (Number of Incidents where the KPI was not in compliance)}}{\text{(Total Severity 1 Incidents where Services for which Contractor is responsible under the SOW are unavailable)}}$$

**Measurement Period:** Calendar Quarter

**Data Source:** Incident Management System Report

**Frequency of Collection:** Calendar Quarter, All Severity 1 and 2 Incidents

**Service Level Measures:**

Individual SL GYR State	Incident Resolution - Incident Triage and Closure and Recidivist Rate
Green	>= 99.5
Yellow	< 99.5 and > =99.3
Red	< 99.3

### 9.9.7. User Interaction – Completion of Administrative, Root, DBA and Privileged User Adds/Deletes

**Business Intent:** Ensure that those individuals (State, Contractor or 3<sup>rd</sup> Party Systems Integrator) that, upon meeting State systems access requirements, are established correctly in the required BI environment(s) to perform their job functions and upon completing their assignment or being relieved of these responsibilities are removed from the system

**Definition:** This SLA shall only apply to those personnel that have administrator (Exa, x86, windows), root or super-user (Unix, Linux or similar), DBA (oracle or file system level) or other elevated or Privileged user access at the operating system or database level prompt. This SLA does not apply to State Authorized users of BI via application level login and use levels.

Completion of Adds/Deletes defines the timeliness of both emergency and scheduled User Deletes.

Emergency is the condition in which, for whatever reason, the State believes there is a real or potential threat or risk to the State for those individuals who have privileged access to BI operating systems, file systems, code, interfaces or database(s) and therefore must be deleted immediately

Late Emergency User Adds/Deletes are defined as anything greater than 1 business hour

Late Scheduled User Adds/Deletes are defined as anything greater than 4 business hours

**Formula:**

$$\frac{\text{Completion of Administrative, Root, DBA and Privileged User Adds/Deletes}}{\frac{((\text{Total Emergency User Adds/Deletes}) - (\text{Late Emergency User Adds/Deletes})) + ((\text{Total Scheduled User Adds/Deletes}) - (\text{Late Scheduled User Adds/Deletes}))}{(\text{Total Emergency User Adds/Deletes}) + (\text{Total Scheduled User Adds/Deletes})}}$$

**Measurement Period:** Month

**Data Source:** Service Desk, Service Request System

**Frequency of Collection:** Daily

**Service Level Measures:**

Individual SL GYR State	Completion of Administrative, Root, DBA and Privileged User Adds/Deletes
Green	>= 99.5
Yellow	>= 98.5 and < 99.5
Red	< 98.5

### 9.9.8. Security – Monitoring & Auditing – Security Breach Detection

**Business Intent:** Ensure that State Security policies are implemented correctly, and monitored and followed at all times for all users of BI whether end-user, State, Contractor or 3<sup>rd</sup> Party

**Definition:** System Security Breach Detection will be determined by monitoring compliance with the following three key performance indicators (KPI):

System security breach success notification due within 30 minutes of physical intrusion detection of any element within the Contractor’s responsibility area or Contractor provided facility or element that accesses BI including Contractor’s machines. Notification will be as set forth in the State/Contractor Process Interface Manual or other supporting documents.

Suspension or Revocation of unapproved or intruder access in accordance with State established procedures within 10 minutes of State approval or (absent State approval) 15 minutes.

System security breach (attempt, failure) notification due within 1 hour of such physical intrusion detection. Notification will be as set forth in the Process Interface Manual or other supporting documents.

**Formula:** Security Breach Detection = 
$$\frac{\text{(Number of instances where individual KPI's were not in compliance)}}{\text{Total Number of Instances}}$$

**Measurement Period:** Month

**Data Sources:** Infrastructure Antivirus/Malware/Rootkit Scan logs, Active Port Scanning Logs, User Account Review Report

**Frequency of Collection:** Monthly

**Service Level Measures:**

Individual SL GYR State	Security Breach Detection
Green	<= 0
Yellow	N/A
Red	> 0

### 9.9.9. Job Schedule and Scheduled Reporting Performance

**Business Intent:** Scheduled Jobs and Reports Start and Complete with established time parameters and execute in such a manner as to not intrude upon online users of BI. Job abends and restarts are monitored and executed within the established schedule.

**Definition:** Job Schedule and Scheduled Reporting Performance shall consider all scheduled daily, weekly, monthly and business cycle Jobs and Reports that execute under the responsibility and scope of the Contractor via UC4 (or successors), automated operating system job schedulers (e.g., cron, task scheduler), PeopleSoft/Oracle job schedulers, Contractor supported ETL data extractions, interfaces and any reports in the Contractor's scope.

The Contractor shall, as part of establishing and maintaining the BI Run Book, establish automated schedules for BI scheduled processes and reports and set Start, Stop and Completion and Job dependencies as appropriate.

The actual Start and Completion of all Scheduled Jobs and Reports shall be recorded on a daily basis as afforded by the automated schedule. For those jobs that cannot be automated for any reason and require Contractor personnel to manually execute these jobs, the actual Start and Stop times shall be recorded and included in the below calculation.

**Formula:**

$$\text{Job Schedule and Scheduled Reporting Performance} = \frac{(\text{Total Number of Minutes Jobs/Reports were delayed from Starting}) + (\text{Total Number of Minutes Jobs/Reports Ran in Excess of Completion/Stop Parameters})}{\text{Total Number of Minutes Jobs/Reports Ran as Scheduled}}$$

**Measurement Period:** Monthly

**Data Sources:** Scheduled Job Report

**Frequency of Collection:** Daily

**Service Level Measures:**

Individual SL GYR State	Job Schedule and Scheduled Reporting Performance
Green	<= 10%
Yellow	> 10% <= 15%
Red	> 15%

## 9.9.10. Operational Process Control & Repeatability – Changes to Production Environments

**Business Intent:** All changes to production environments follow a disciplined process, are authorized by the State and documentation is updated at all times to ensure that the operating environment of BI is up to date and documentation is current. Production changes are tested/validated and move as a comprehensive change package as opposed to piecemeal elements that result in unintended consequences.

**Definition:** The changes to production environment measure is determined by monitoring compliance with the following six key performance indicators:

1. All changes to production environments have an authorization from an approved the State employee
2. Code or System changes are promoted to production environments that use contemporary change control methods including version control, data backup/back out procedures (if applicable)
3. All elements that comprise a system change inclusive of code, configuration values, environment parameters, database elements, PeopleTools, PS-Admin, security, executables and other required change elements are applied as part of a Production change.
4. No untested or unapproved changes or changed elements that are not required by a production change are introduced into the production environment
5. Changes that are detected to introduce errors or unavailability to production systems are reversed in accordance with the Contractor back-out procedure and the system is restored to the pre-change state without impacting regular operations
6. Corresponding updates to the Process Interface Manual and other supporting documents are completed within three business days of receiving and implementing minor approved change request(s).

**Formula:** 
$$\frac{\text{Changes to Production Environments}}{\text{Total Number of KPIs met}} = \frac{\text{Total Number of KPIs not met}}{\text{Total Number of KPIs met}}$$

**Measurement Period:** Monthly

**Data Sources:** Production Change Report

**Frequency of Collection:** Each Change to Production

**Service Level Measures:**

Individual SL GYR State	Changes to Production Environments
Green	<= 1%
Yellow	> 1% <= 3%
Red	> 3%

### 9.9.11. Service Quality – System Changes

**Business Intent:** System Changes are implemented correctly the first time, and do not cause unintended consequences to BI users, scheduled jobs and reports, corrupt or compromise data or data relationships and otherwise perform as intended from a functional, technical and performance perspective. Non-Production environments reflect Production.

**Definition:** The Service Quality System Changes measure is determined by monitoring compliance with the following four key performance indicators (KPI):

1. System changes or updates (i.e., break fix, configuration, and patches) in any release to production environment are implemented correctly the first time inclusive of all code, non-code, configuration, interface, scheduled job or report, database element or other change to the production environment
2. System changes or updates are propagated within 5 business days as mutually deemed appropriate to non-production environments such that environment configurations are synchronized and reflect the then current environment and a common development, testing, QA, demonstration and training environment is carried forward that is reflective of production
3. Production system changes (i.e., break fix, configuration, and patches) in releases that do not cause other problems
4. System changes or updates (i.e., break fix, configuration, and patches) in emergency releases are implemented correctly the first time that comprise the BI system

**Formula:** Service Quality – System Changes = 
$$\frac{\text{Total Number of KPIs not met}}{\text{Total Number of KPIs met}}$$

**Measurement Period:** Monthly

**Data Sources:** Production Change Report

**Frequency of Collection:** Each Change to Production and Follow-On Changes to Non-Production

**Service Level Measures:**

Individual SL GYR State	Service Quality – System Changes
Green	<= 2%
Yellow	> 2% <= 5%
Red	> 5%

## 9.9.12. Service Timeliness – System Changes

**Business Intent:** System Changes are implemented in a timely manner as scheduled with the State or (if applicable) during a Scheduled Maintenance Period or as required by the State

**Definition:** The Service Timeliness System Changes measure is determined by monitoring compliance with the following two key performance indicators (KPI):

1. Emergency system changes or updates (i.e., break fix, configuration, and patches) to BI will be initiated within 24 hours of the State approved request and Change Management Process and to be reported complete within 1 hour of completion
2. Non-emergency system changes or updates (i.e., break fix, configuration, and patches) to BI to be initiated in accordance with the State policies during a scheduled maintenance period or as mutually scheduled between the Contractor and State and reported within 2 days of post implementation certification

**Formula:**

$$\text{Service Quality – System Change Timeliness} = \frac{\text{Total Number of KPIs not in Compliance in a Month}}{\text{Total Number of System Changes in a Month}}$$

**Measurement Period:** Monthly

**Data Sources:** Production Change Report

**Frequency of Collection:** Each Change to Production and Follow-On Changes to Non-Production

**Service Level Measures:**

Individual SL GYR State	Service Quality – System Changes
Green	<= 2%
Yellow	> 2% <= 5%
Red	> 5%

### 9.9.13. Data Accuracy

**Business Intent:** Ensure that all data in the Business Intelligence target environment is consistent with the source.

**Definition:** Contractor must resolve all data accuracy issues/validation failures in the Business Intelligence Environment within seven (7) days of repairing source data within each occurrence. Data accuracy issues arising directly from the Contractor activities or personnel must be resolved within two (2) days of identification by either the State or Contractor. The Contractor shall not be penalized for inaccuracies for which the resolution was prohibited by another party (e.g. actions of the State or another State vendor).

**Formula:** 
$$\text{Data Accuracy Instances} = \frac{\text{Number of instances where data accuracy issues/validation is not resolved timely as stated in definition above}}{\text{Total Number of Instances}}$$

**Measurement Period:** Monthly

**Data Sources:** Business Intelligence target environment and corresponding source environment

**Frequency of Collection:** Monthly

**Service Level Measures:**

Individual SL GYR State	Service Quality – System Changes
Green	= 0
Yellow	= 1 or 2
Red	> 2

# Supplement 2:

## Enterprise Business Intelligence Operations & Project Services

State Architecture and Computing Standards Requirements  
State Security and Privacy Requirements  
State IT Computing Policy Requirements  
State Data Handling Requirements

## Contents

State Architecture and Computing Standards Requirements.....	1
State Security and Privacy Requirements .....	1
State IT Computing Policy Requirements .....	1
State Data Handling Requirements .....	1
<b>1. Overview and Scope .....</b>	<b>4</b>
<b>2. State Architecture and Computing Standards Requirements.....</b>	<b>4</b>
2.1. Requirements Overview .....	4
2.1.1. State of Ohio Standards .....	4
2.1.2. Offeror Responsibilities .....	4
2.2. Compute Requirements: Client Computing.....	4
2.2.1. Compute Requirements: Server / OS.....	5
2.2.2. Ohio Cloud: Hypervisor Environment .....	5
2.3. Storage and Backup Requirements .....	5
2.3.1. Storage Pools.....	5
2.3.2. Backup .....	6
2.4. Networking Requirements: Local Area Network (LAN) / Wide Area Network (WAN) .....	6
2.5. Application Requirements .....	6
2.5.1. Application Platforms.....	6
2.5.2. Open API's .....	6
2.5.3. SOA (Service Oriented Architecture) .....	6
2.6. Database Platforms.....	7
2.7. Enterprise Application Services.....	7
2.7.1. Health and Human Services: Integrated Eligibility .....	7
2.7.2. The Ohio Business Gateway (OBG) .....	7
2.7.3. Ohio Administrative Knowledge System (OAKS).....	8
2.7.4. Enterprise Business Intelligence .....	9
2.7.5. SharePoint.....	9
2.7.6. IT Service Management .....	9
2.7.7. Enterprise Geocoding Services.....	9
2.7.8. GIS Hosting.....	9
2.8. Productivity, Administrative and Communication Requirements.....	10
2.8.1. Communication Services.....	10
<b>3. General State Security and Information Privacy Standards and Requirements.....</b>	<b>11</b>
3.1. State Provided Elements: Contractor Responsibility Considerations.....	11
3.2. Periodic Security and Privacy Audits.....	12
3.3. Annual Security Plan: State and Contractor Obligations.....	13
3.4. State Network Access (VPN) .....	13
3.5. Security and Data Protection.....	14
3.6. State Information Technology Policies.....	14
<b>4. State and Federal Data Privacy Requirements.....</b>	<b>15</b>
4.1. Protection of State Data .....	15
4.2. Handling the State's Data.....	16
4.3. Contractor Access to State Networks Systems and Data .....	17
4.4. Portable Devices, Data Transfer and Media .....	18
4.5. Limited Use; Survival of Obligations.....	18

4.6.	Disposal of PI/SSI .....	18
4.7.	Remedies .....	18
4.8.	Prohibition on Off-Shore and Unapproved Access .....	18
4.9.	Background Check of Contractor Personnel .....	19
4.10.	Federal Tax Information .....	19
<b>5.</b>	<b>Contractor Responsibilities Related to Reporting of Concerns, Issues and Security/Privacy Issues .....</b>	<b>21</b>
5.1.	General.....	21
5.2.	Actual or Attempted Access or Disclosure .....	21
5.3.	Unapproved Disclosures and Intrusions: Contractor Responsibilities.....	22
5.4.	Security Breach Reporting and Indemnification Requirements.....	22
<b>6.</b>	<b>Security Review Services .....</b>	<b>22</b>
6.1.	Hardware and Software Assets.....	22
6.2.	Security Standards by Device and Access Type .....	23
6.3.	Boundary Defenses.....	23
6.4.	Audit Log Reviews.....	23
6.5.	Application Software Security.....	23
6.6.	System Administrator Access.....	23
6.7.	Account Access Privileges .....	24
6.8.	Additional Controls and Responsibilities .....	24

## 1. Overview and Scope

This Supplement shall apply to any and all Work, Services, Locations and Computing Elements that the Contractor will perform, provide, occupy or utilize in conjunction with the delivery of work to the State and any access of State resources in conjunction with delivery of work.

This scope shall specifically apply to:

- Major and Minor Projects, Upgrades, Updates, Fixes, Patches and other Software and Systems inclusive of all State elements or elements under the Contractor's responsibility utilized by the State;
- Any systems development, integration, operations and maintenance activities performed by the Contractor;
- Any authorized Change Orders, Change Requests, Statements of Work, extensions or Amendments to this agreement;
- Contractor locations, equipment and personnel that access State systems, networks or data directly or indirectly; and
- Any Contractor personnel, or sub-Contracted personnel that have access to State confidential, personal, financial, infrastructure details or sensitive data.

The terms in this Supplement are additive to the Standard State Terms and Conditions contained elsewhere in this agreement. In the event of a conflict for whatever reason, the highest standard contained in this agreement shall prevail.

## 2. State Architecture and Computing Standards Requirements

### 2.1. Requirements Overview

Offerors responding to State issued RFQ / RFP requests, and as Contractors performing the work following an award are required to propose solutions that comply with the standards outlined in this document. In the event of a conflict with any published Standard, a variance may be requested, and the Offeror must show sufficient business justification for the variance request. The Enterprise IT Architecture Team will engage with the Contractor and appropriate State stakeholders to review and approve / deny the variance request.

#### 2.1.1. State of Ohio Standards

The State has a published Core Technology Stack as well as Enterprise Design Standards as outlined in this document and, due to State preferences, are subject to improvements, elaboration and replacement. The State also provides numerous IT Services in both the Infrastructure and Application categories, as outlined in the State's IT Services Catalog at: <http://das.ohio.gov/Divisions/InformationTechnology/StateofOhioITServiceCatalog.aspx>

#### 2.1.2. Offeror Responsibilities

Offerors can propose on-premise or cloud-based solutions. When proposing on-premise solutions, vendors must comply with State requirements including using the State's Virtualized Compute Platform. Offerors proposing on-premise solutions are required to install third party applications on State provided compute platforms. Dedicated server platforms are not compliant with the State's Virtualization Requirements.

In addition, Offerors are required to take advantage of all published IT Application Services where possible, i.e. Enterprise Service Bus, Content Management, Enterprise Document Management, Data Warehousing, Data Analytics and Reporting and Business Intelligence. When dedicated Application components are required, i.e. Application Servers, Databases, etc., they should comply with the Core Technology standards.

## 2.2. Compute Requirements: Client Computing

Offerors **must not** propose solutions that require custom PC's, Laptops, Notebooks etc. The State will source its own Client computing hardware and the Offeror's proposed solutions are required to be compatible with the State's hardware.

### 2.2.1. Compute Requirements: Server / OS

Offerors **must** propose solutions that comply with the State's supported Server / OS versions.

The following are the State's Required Server and OS versions.

**Table 1 – Supported Server/OS versions**

Operating System	Version	Edition
Microsoft Windows Server	2012, 2012 R2	Standard, Enterprise, & Datacenter
RedHat Linux	7	Enterprise
SUSE Linux	11	Enterprise
IBM AIX	7.1	
Oracle Enterprise Linux		Enterprise

When Offerors are proposing on-premise solutions, these solutions must comply with the State's supported Server Compute Platforms.

The State hosts and manages the Virtual Server hardware and Virtualization layer. The State is also responsible for managing the server's Operating System (OS). This service includes 1 virtual CPU (vCPU), 1 GB of RAM and 50 GB of Capacity Disk Storage. Customers can request up to 8 vCPUs and 24GB of RAM.

For Ohio Benefits and the Ohio Administrative Knowledge System (OAKS) – Exalogic Version 2.0.6.0.2

### 2.2.2. Ohio Cloud: Hypervisor Environment

When Offerors are proposing on-premise solutions, these solutions *must* comply with the State's supported VMware vSphere, and IBM Power Hypervisor environment.

For Ohio Benefits and OAKS – Oracle Virtual Manager Version 3.3.1, Xen

## 2.3. Storage and Backup Requirements

### 2.3.1. Storage Pools

The State provides three pools (tiers) of storage with the ability to use and allocate the appropriate storage type based on predetermined business criticality and requirements. Storage pools are designed to support different I/O workloads.

When Offerors are proposing on-premise solutions, these solutions *must* take advantage of the State's Storage Service Offerings.

For Ohio Benefits and OAKS - HA (High Availability) storage used with Mirror configuration.

The pools and their standard use cases are below:

Table 2 – State Supported Storage Pools

Storage Pool	Availability	Performance	Typical Applications
Performance	Highest	Fast	Performance pool suited for high availability applications, with high I/O (databases).
General	High	Fast	General pool suitable for file servers, etc.
Capacity	High	Average	Capacity pool suitable for file servers, images and backup / archive). Not suited for high random I/O.

### 2.3.2. Backup

When Offerors are proposing on-premise solutions, these solutions *must* take advantage of the State's Backup Service Offering.

Backup service uses IBM Tivoli Storage Manager Software and provides for nightly backups of customer data. It also provides for necessary restores due to data loss or corruption. The option of performing additional backups, archiving, restoring or retrieving functions is available for customer data. OIT backup facilities provide a high degree of stability and recoverability as backups are duplicated to the alternate site.

For Ohio Benefits - Symantec NetBackup is the Enterprise backup solution.

## 2.4. Networking Requirements: Local Area Network (LAN) / Wide Area Network (WAN)

Offerors **must** propose solutions that work within the State's LAN / WAN infrastructure.

The State of Ohio's One Network is a unified solution that brings together Design, Engineering, Operations, Service Delivery, Security, Mobility, Management, and Network Infrastructure to target and solve key Government challenges by focusing on processes, procedures, consistency and accountability across all aspects of State and Local Government.

Ohio One Network can deliver an enterprise network access experience for their customers regardless of location or device and deliver a consistent, reliable network access method.

The State provides a high bandwidth internal network for internal applications to communicate across the State's LAN / WAN infrastructure. Normal traffic patterns at major sites should be supported.

Today, the State's WAN (OARnet) consists of more than 1,850 miles of fiber-optic backbone, with more than 1,500 miles of it operating at ultrafast 100 Gbps speeds. The network blankets the state, providing connectivity to all State Government Agencies.

The State of Ohio Network infrastructure utilizes private addressing, reverse proxy technology and Network Address Translation (NAT). All applications that are to be deployed within the infrastructure must be tolerant of these technologies for both internal product interaction as well as external user access to the proposed system, infrastructure or application.

The State Network team will review applications requirements involving excessive bandwidth (i.e. voice, video, telemetry, or applications) deployed at remote sites.

## 2.5. Application Requirements

### 2.5.1. Application Platforms

When Offerors are proposing on-premise solutions, these solutions *must* be developed in open or industry standard languages (e.g. Java, .NET, PHP, etc.)

### 2.5.2. Open API's

Proposed vendor applications must be developed with standards-based Open API's. An open API is an [application program interface](#) that provides programmatic access to software applications. Proposed vendor applications must describe in detail all available features and functionality accessible via APIs.

### 2.5.3. SOA (Service Oriented Architecture)

When Offerors are proposing on-premise solutions, these solutions *must* be developed using a standards-based Service Oriented Architecture (SOA) model.

## 2.6. Database Platforms

Proposed vendor application designs must run on databases that comply with the State's supported Database Platforms.

- DB2 Version 10
- SQL 2012 or higher
- ORACLE 11g and 12C
- Exadata Version 11.2.3.2.1

## 2.7. Enterprise Application Services

The State of Ohio Office of Information Technology (OIT) provides a number of Enterprise Shared Services to State agencies as outline in the IT Services Catalog available at:

<http://das.ohio.gov/Divisions/InformationTechnology/StateofOhioITServiceCatalog.aspx>

At a minimum, proposed vendor application designs that include the following Application Services *must* use the Application IT Services outlined in the IT Services Catalog.

### 2.7.1. Health and Human Services: Integrated Eligibility

The Integrated Eligibility Enterprise platform provides four key distinct technology domains / capabilities:

- Common Enterprise Portal – includes User Interface and User Experience Management, Access Control, Collaboration, Communications and Document Search capability
- Enterprise Information Exchange – includes Discovery Services (Application and Data Integration, Master Data Management (MDM) Master Person Index and Record Locator Service), Business Process Management, Consent Management, Master Provider Index and Security Management
- Analytics and Business Intelligence – Integration, Analysis and Delivery of analytics in the form of alerts, notifications and reports
- Integrated Eligibility – A common Enterprise Application framework and Rules Engine to determine eligibility and benefits for Ohio Public Benefit Programs

### 2.7.2. The Ohio Business Gateway (OBG)

The Ohio Business Gateway (OBG) offers Ohio's businesses a time-and money-saving online filing and payment system that helps simplify business' relationship with Government agencies.

- New Business Establishment – Provides a single, portal based web location for the establishment of new businesses in Ohio, file with the required State agencies and ensure that business compliance requirements of the State are met.
- Single Point Revenue and Fee Collection - Manage payments to State's payment processor (CBOSS) and broker payment to multiple agencies while creating transaction logs and Business Customer "receipts".
- One-Stop Filing and Forms - Provides guides and forms to Business Users through complex transactions that have multiple steps, forms and / or filing requirements for users on procedures to complete the process including Agencies and (if applicable) systems they will need to interact with.
- Scheduling and Reminders - Notify Business Customers of a particular event that is upcoming or past due (Filing due) using a "calendar" or "task list" metaphor.

- Collections and Confirmations – Provides a Payment Card Industry (PCI) certified web-based payment solution that supports a wide range of payment types: credit cards, debit cards, electronic checks, as well as recurring, and cash payments.

### **2.7.3. Ohio Administrative Knowledge System (OAKS)**

OAKS is the State's Enterprise Resource Planning (ERP) system, which provides central administrative business services such as Financial Management, Human Capital Management, Content Management via myOhio.gov, Enterprise Learning Management, and Customer Relationship Management. Core System Capabilities include (but are not limited to):

#### **Content Management (myohio.gov)**

- Centralized Communications to State Employees and State Contractors
- OAKS alerts, job aids, and news
- Statewide Top Stories
- Portal to OAKS applications
- Employee and Contractor Management

#### **Enterprise Business Intelligence**

- Key Financial and Human Resources Data, Trends and Analysis
- Cognos driven standardized and adhoc reporting

#### **Financial Management (FIN)**

- Accounts Payable
- Accounts Receivable
- Asset Management
- Billing
- eBid
- eCatalog (Ohio Marketplace)
- eInvoicing (coming Fall 2015)
- eSupplier/Offeror Maintenance
- Financial Reporting
- General Ledger
- Planning and Budgeting
- Procurement
- Travel & Expense

#### **Customer Relationship Management (CRM)**

- Contact / Call Center Management

#### **Enterprise Learning Management (ELM)**

- Training Curriculum Development
- Training Content Delivery

#### **Human Capital Management (HCM)**

- Benefits Administration

- Payroll
- Position Management
- Time and Labor
- Workforce Administration: Employee and Contingent Workers
- Employee Self-Service
- eBenefits
- ePerformance
- Payroll

#### 2.7.4. Enterprise Business Intelligence

- Health and Human Services Information
  - Eligibility
    - Operational Metrics
    - County Caseworker Workload
  - Claims [Q1, 2015]
  - Long Term Care [Q2, 2015]
- Financial Information
  - General Ledger (Spend, Disbursement, Actual/Forecast)
  - Travel and Expense
  - Procure to Pay (AP/PO/Offeror/Spend)
  - Capital Improvements
  - Accounts Receivable
  - Asset Management
- Workforce and Human Resources
  - Workforce Profile
  - Compensation
  - MBE/EDGE

#### 2.7.5. SharePoint

Microsoft SharePoint Server 2013 portal setup and hosting services for agencies interested in internal collaboration, external collaboration, organizational portals, business process workflow, and business intelligence. The service is designed to provision, operate and maintain the State's enterprise Active Directory Accounts.

#### 2.7.6. IT Service Management

ServiceNow, a cloud-based IT Service Management Tool that provides internal and external support through an automated service desk workflow based application which provides flexibility and ease of use. The IT Service Management Tool provides workflows aligning with ITIL processes such as Incident Management, Request Fulfillment, Problem Management, Change Management and Service Catalog.

#### 2.7.7. Enterprise Geocoding Services

Enterprise Geocoding Services (EGS) combine address standardization, geocoding, and spatial analysis into a single service. Individual addresses can be processed in real time for on line applications or large numbers of addresses can be processed in batch mode.

#### 2.7.8. GIS Hosting

GIS Hosting delivers dynamic maps, spatial content, and spatial analysis via the Internet. User agencies can integrate enterprise-level Geographic Information Systems (GIS) with map capabilities and spatial content into new or existing websites and applications.

## **2.8. Productivity, Administrative and Communication Requirements**

### **2.8.1. Communication Services**

The State of Ohio Office of Information Technology (OIT) provides a number of Enterprise Shared Services to State agencies as outline in the IT Services Catalog available at:

<http://das.ohio.gov/Divisions/InformationTechnology/StateofOhioITServiceCatalog.aspx>

At a minimum, proposed vendor application designs that include the following Communication Services **must** use the Communication Services outlined in the IT Services Catalog.

#### **Exchange**

- Exchange Mail
- Office 365
- Skype for Business Instant Messaging & Presence
- Enterprise Vault
- Clearwell eDiscovery
- Exchange Web Services
- Bulk Mailing
- External Mail Encryption
- Outbound Fax
- Mobile devices

#### **EDI/Application Integration/Medicaid EDI**

#### **Lyris Listserv**

#### **On-premise application based FAX: eFAX**

Fax2Mail is a “hosted” fax solution that allows agencies to seamlessly integrate inbound and outbound Fax with their existing desktop E-mail and back-office environments. Fax2Mail is a “cloud-based” solution.

#### **Voice over Internet Protocol (VoIP)**

#### **Audio Conference**

#### **Video Conference**

#### **Call Centers**

### 3. General State Security and Information Privacy Standards and Requirements

The Contractor will be responsible for maintaining information security in environments under the Contractor's management and in accordance with State IT Security Policies. The Contractor will implement an information security policy and security capability as set forth in this agreement.

The Contractor's responsibilities with respect to Security Services will include the following:

- Provide vulnerability management Services for the Contractor's internal secure network connection, including supporting remediation for identified vulnerabilities as agreed.
- Support the implementation and compliance monitoring for State IT Security Policies.
- Develop, maintain, update, and implement security procedures, with State review and approval, including physical access strategies and standards, ID approval procedures and a breach of security action plan.
- Manage and administer access to the systems, networks, System software, systems files and State data, excluding end-users.
- Provide support in implementation of programs to educate State and Contractor end-users and staff on security policies and compliance.
- Install and update Systems software security, assign and reset passwords per established procedures, provide the State access to create User ID's, suspend and delete inactive logon IDs, research system security problems, maintain network access authority, assist in processing State security requests, perform security reviews to confirm that adequate security procedures are in place on an ongoing basis, and provide incident investigation support (jointly with the State ), and provide environment and server security support and technical advice.
- Develop, implement, and maintain a set of automated and manual processes to ensure that data access rules are not compromised.
- Perform physical security functions (e.g., identification badge controls, alarm responses) at the facilities under the Contractor's control.
- Prepare an Information Security Controls Document. This document is the security document that is used to capture the security policies and technical controls that the Contractor will implement, as requested by the State, on Contractor managed systems, supported servers and the LAN within the scope of this agreement. The Contractor will submit a draft document for State review and approval during the transition period.

The State will:

- Develop, maintain and update the State IT Security Policies, including applicable State information risk policies, standards and procedures.
- Provide a State Single Point of Contact with responsibility for account security audits;
- Support intrusion detection and prevention and vulnerability scanning pursuant to State IT Security Policies;
- Provide the State security audit findings material for the Services based upon the security policies, standards and practices in effect as of the Effective Date and any subsequent updates.
- Assist the Contractor in performing a baseline inventory of access IDs for the systems for which the Contractor has security responsibility;
- Authorize User IDs and passwords for the State personnel for the Systems software, software tools and network infrastructure systems and devices under Contractor management;
- Approve non-expiring passwords and policy exception requests, as appropriate.

#### 3.1. State Provided Elements: Contractor Responsibility Considerations

The State is responsible for Network Layer (meaning the internet Protocol suite and the open systems interconnection model of computer networking protocols and methods to process communications across the IP

network) system services and functions that build upon State infrastructure environment elements, the Contractor shall not be responsible for the implementation of Security Services of these systems as these shall be retained by the State.

To the extent that Contractor's access or utilize State provided networks, the Contractor is responsible for adhering to State policies and use procedures and do so in a manner as to not diminish established State capabilities and standards.

The Contractor will be responsible for maintaining the security of information in environment elements that it accesses, utilizes, develops or manages in accordance with the State Security Policy. The Contractor will implement information security policies and capabilities, upon review and agreement by the State, based on the Contractor's standard service center security processes that satisfy the State's requirements contained herein.

The Contractor's responsibilities with respect to security services must also include the following:

- Support intrusion detection & prevention including prompt agency notification of such events, reporting, monitoring and assessing security events.
- Provide vulnerability management services including supporting remediation for identified vulnerabilities as agreed.
- Support the State IT Security Policy which includes the development, maintenance, updates, and implementation of security procedures with the agency's review and approval, including physical access strategies and standards, ID approval procedures and a breach of security action plan.
- Support OIT in the implementation, maintenance and updating of statewide data security policies, including the State information risk policies, standards and procedures.
- Managing and administering access to the systems, networks, Operating Software or System Software, (including programs, device drivers, microcode and related code supporting documentation and media that: 1) perform tasks basic to the functioning of data processing and network connectivity; and 2) are required to operate Applications Software), systems files and the State Data.
- Supporting the State in implementation of programs to raise the awareness of End Users and staff personnel as to the existence and importance of security policy compliance.
- Installing and updating State provided or approved system security Software, assigning and resetting passwords per established procedures, providing the agency access to create user ID's, suspend and delete inactive logon IDs, research system security problems, maintain network access authority, assisting in processing the agency requested security requests, performing security audits to confirm that adequate security procedures are in place on an ongoing basis, with the agency's assistance providing incident investigation support, and providing environment and server security support and technical advice.
- Developing, implementing, and maintaining a set of automated and manual processes so that the State data access rules, as they are made known by the State, are not compromised.
- Performing physical security functions (e.g., identification badge controls, alarm responses) at the facilities under Contractor control.

### **3.2. Periodic Security and Privacy Audits**

The State shall be responsible for conducting periodic security and privacy audits and generally utilizes members of the OIT Chief Information Security Officer and Privacy teams, the OBM Office of Internal Audit and the Auditor of State, depending on the focus area of an audit. Should an audit issue or finding be discovered the following resolution path shall apply:

- If a security or privacy issue is determined to be pre-existing to this agreement, the State will have responsibility to address or resolve the issue. Dependent on the nature of the issue the State may elect to contract with the Contractor under mutually agreeable terms for those specific resolution services at that time or elect to address the issue independent of the Contractor.
- For in-scope environments and services, all new systems implemented or deployed by the Contractor shall comply with State security and privacy policies.

### 3.3. Annual Security Plan: State and Contractor Obligations

The Contractor will develop, implement and thereafter maintain annually a Security Plan for review, comment and approval by the State Information Security and Privacy Officer, that a minimum must include and implement processes for the following items related to the system and services:

- Security policies
- Logical security controls (privacy, user access and authentication, user permissions, etc.)
- Technical security controls and security architecture (communications, hardware, data, physical access, software, operating system, encryption, etc.)
- Security processes (security assessments, risk assessments, incident response, etc.)
- Detail the technical specifics to satisfy the following:
  - Network segmentation
  - Perimeter security
  - Application security and data sensitivity classification
  - PHI and PII data elements
  - Intrusion management
  - Monitoring and reporting
  - Host hardening
  - Remote access
  - Encryption
  - State-wide active directory services for authentication
  - Interface security
  - Security test procedures
  - Managing network security devices
  - Security patch management
  - Detailed diagrams depicting all security-related devices and subsystems and their relationships with other systems for which they provide controls
  - Secure communications over the Internet

The Security Plan must detail how security will be controlled during the implementation of the System and Services and contain the following:

- High-level description of the program and projects
- Security risks and concerns
- Security roles and responsibilities
- Program and project security policies and guidelines
- Security-specific project deliverables and processes
- Security team review and approval process
- Security-Identity management and Access Control for Contractor and State joiners, movers, and leavers
- Data Protection Plan for personal/sensitive data within the projects
- Business continuity and disaster recovery plan for the projects
- Infrastructure architecture and security processes
- Application security and industry best practices for the projects
- Vulnerability and threat management plan (cyber security)

### 3.4. State Network Access (VPN)

Any remote access to State systems and networks, Contractor or otherwise, must employ secure data transmission protocols, including the secure sockets layer (SSL) protocol and public key authentication, signing and encryption. In addition, any remote access solution must use Secure Multipurpose Internet Mail Extensions (S/MIME) to provide encryption and non-repudiation services through digital certificates and the provided PKI. Multi-factor authentication is to be employed for users with privileged network access by leveraging the State of Ohio RSA solution.

### 3.5. Security and Data Protection.

All Services must also operate at the [moderate level baseline] as defined in the National Institute of Standards and Technology (“NIST”) 800-53 Rev. 3 [moderate baseline requirements], be consistent with Federal Information Security Management Act (“FISMA”) requirements, and offer a customizable and extendable capability based on open-standards APIs that enable integration with third party applications. Additionally, they must provide the State’s systems administrators with 24x7 visibility into the services through a real-time, web-based “dashboard” capability that enables them to monitor, in real or near real time, the Services’ performance against the established SLAs and promised operational parameters.

### 3.6. State Information Technology Policies

The Contractor is responsible for maintaining the security of information in environment elements under direct management and in accordance with State Security policies and standards. The Contractor will implement information security policies and capabilities as set forth in Statements of Work and, upon review and agreement by the State, based on the Offeror’s standard service center security processes that satisfy the State’s requirements contained herein. The Offeror’s responsibilities with respect to security services include the following:

- Support intrusion detection & prevention including prompt agency notification of such events, reporting, monitoring and assessing security events.
- Support the State IT Security Policy which includes the development, maintenance, updates, and implementation of security procedures with the agency’s review and approval, including physical access strategies and standards, ID approval procedures and a breach of security action plan.
- Managing and administering access to the Operating Software, systems files and the State Data.
- Installing and updating State provided or approved system security Software, assigning and resetting administrative passwords per established procedures, providing the agency access to create administrative user ID’s, suspending and deleting inactive logon IDs, researching system security problems, maintaining network access authority, assist processing of the agency requested security requests, performing security audits to confirm that adequate security procedures are in place on an ongoing basis, with the agency’s assistance providing incident investigation support, and providing environment and server security support and technical advice.
- Developing, implementing, and maintaining a set of automated and manual processes so that the State data access rules are not compromised.
- Where the Contractor identifies a potential issue in maintaining an “as provided” State infrastructure element with the more stringent requirement of an agency security policy (which may be federally mandated or otherwise required by law), identifying to agencies the nature of the issue, and if possible, potential remedies for consideration by the State agency.
- The State shall be responsible for conducting periodic security and privacy audits and generally utilizes members of the OIT Chief Information Security Officer and Privacy teams, the OBM Office of Internal Audit and the Auditor of State, depending on the focus area of an audit. Should an audit issue be discovered the following resolution path shall apply:
- If a security or privacy issue is determined to be pre-existing to this agreement, the State will have responsibility to address or resolve the issue. Dependent on the nature of the issue the State may elect to contract with the Contractor under mutually agreeable terms for those specific resolution services at that time or elect to address the issue independent of the Contractor.

- If over the course of delivering services to the State under this Statement of Work for in-scope environments the Contractor becomes aware of an issue, or a potential issue that was not detected by security and privacy teams the Contractor is to notify the State within two (2) hours. This notification shall not minimize the more stringent Service Level Agreements pertaining to security scans and breaches contained herein, which due to the nature of an active breach shall take precedence over this notification. Dependent on the nature of the issue the State may elect to contract with the Contractor under mutually agreeable terms for those specific resolution services at that time or elect to address the issue independent of the Contractor.
- For in-scope environments and services, all new systems implemented or deployed by the Contractor shall comply with State security and privacy policies.

The Contractor will comply with State Security and Privacy policies and standards. For purposes of convenience, a compendium of links to this information is provided in the Table below.

### State of Ohio Security and Privacy Policies

Item	Link
Statewide IT Standards	<a href="http://das.ohio.gov/Divisions/InformationTechnology/StateofOhioITStandards.aspx">http://das.ohio.gov/Divisions/InformationTechnology/StateofOhioITStandards.aspx</a>
Statewide IT Bulletins	<a href="http://das.ohio.gov/Divisions/InformationTechnology/StateofOhioITBulletins.aspx">http://das.ohio.gov/Divisions/InformationTechnology/StateofOhioITBulletins.aspx</a>
IT Policies and Standards	<a href="http://das.ohio.gov/Divisions/InformationTechnology/StateofOhioITPolicies/tabid/107/Default.aspx">http://das.ohio.gov/Divisions/InformationTechnology/StateofOhioITPolicies/tabid/107/Default.aspx</a>
DAS Standards (Computing and??)	100-11 Protecting Privacy), (700 Series – Computing) and (2000 Series – IT Operations and Management) <a href="http://das.ohio.gov/Divisions/DirectorsOffice/EmployeeServices/DASpolicies/tabid/463/Default.aspx">http://das.ohio.gov/Divisions/DirectorsOffice/EmployeeServices/DASpolicies/tabid/463/Default.aspx</a>

## 4. State and Federal Data Privacy Requirements

Because the privacy of individuals’ personally identifiable information (PII) and State Sensitive Information, generally information that is not subject to disclosures under Ohio Public Records law, (SSI) is a key element to maintaining the public’s trust in working with the State, all systems and services shall be designed and shall function according to the following fair information practices principles. To the extent that personally identifiable information in the system is “protected health information” under the HIPAA Privacy Rule, these principles shall be implemented in alignment with the HIPAA Privacy Rule. To the extent that there is PII in the system that is not “protected health information” under HIPAA, these principles shall still be implemented and, when applicable, aligned to other law or regulation.

All parties to this agreement specifically agree to comply with state and federal confidentiality and information disclosure laws, rules and regulations applicable to work associated with this RFP including but not limited to:

- United States Code 42 USC 1320d through 1320d-8 (HIPAA);
- Code of Federal Regulations, 42 CFR 431.300, 431.302, 431.305, 431.306, 435.945, 45 CFR 164.502 (e) and 164.504 (e);
- Ohio Revised Code, ORC 173.20, 173.22, 1347.01 through 1347.99, 2305.24, 2305.251, 3701.243, 3701.028, 4123.27, 5101.26, 5101.27, 5101.572, 5112.21, and 5111.61; and
- Corresponding Ohio Administrative Code Rules and Updates.
- Systems and Services must support and comply with the State’s security operational support model which is aligned to NIST 800-53 Revision 3.

### 4.1. Protection of State Data

**Protection of State Data.** To protect State Data as described in this agreement, in addition to its other duties regarding State Data, Contractor will:

- Maintain in confidence any personally identifiable information (“PI”) and State Sensitive Information (“SSI”) it may obtain, maintain, process, or otherwise receive from or through the State in the course of the Agreement;
- Use and permit its employees, officers, agents, and independent contractors to use any PI/SSI received from the State solely for those purposes expressly contemplated by the Agreement;
- Not sell, rent, lease or disclose, or permit its employees, officers, agents, and independent contractors to sell, rent, lease, or disclose, any such PI/SSI to any third party, except as permitted under this Agreement or required by applicable law, regulation, or court order;
- Take all commercially reasonable steps to (a) protect the confidentiality of PI/SSI received from the State and (b) establish and maintain physical, technical and administrative safeguards to prevent unauthorized access by third parties to PI/SSI received by Contractor from the State;
- Give access to PI/SSI of the State only to those individual employees, officers, agents, and independent contractors who reasonably require access to such information in connection with the performance of Contractor’s obligations under this Agreement;
- Upon request by the State, promptly destroy or return to the State in a format designated by the State all PI/SSI received from the State;
- Cooperate with any attempt by the State to monitor Contractor’s compliance with the foregoing obligations as reasonably requested by the State from time to time. The State shall be responsible for all costs incurred by Contractor for compliance with this provision of this subsection;
- Establish and maintain data security policies and procedures designed to ensure the following:
  - a) Security and confidentiality of PI/SSI;
  - b) Protection against anticipated threats or hazards to the security or integrity of PI/SSI; and
  - c) Protection against the unauthorized access or use of PI/SSI.

#### 4.1.1. Disclosure

**Disclosure to Third Parties.** This Agreement shall not be deemed to prohibit disclosures in the following cases:

- Required by applicable law, regulation, court order or subpoena; provided that, if the Contractor or any of its representatives are ordered or requested to disclose any information provided by the State, whether PI/SSI or otherwise, pursuant to court or administrative order, subpoena, summons, or other legal process, Contractor will promptly notify the State (unless prohibited from doing so by law, rule, regulation or court order) in order that the State may have the opportunity to seek a protective order or take other appropriate action. Contractor will also cooperate in the State’s efforts to obtain a protective order or other reasonable assurance that confidential treatment will be accorded the information provided by the State. If, in the absence of a protective order, Contractor is compelled as a matter of law to disclose the information provided by the State, Contractor may disclose to the party compelling disclosure only the part of such information as is required by law to be disclosed (in which case, prior to such disclosure, Contractor will advise and consult with the State and its counsel as to such disclosure and the nature of wording of such disclosure) and Contractor will use commercially reasonable efforts to obtain confidential treatment therefore;
- To State auditors or regulators;
- To service providers and agents of either party as permitted by law, provided that such service providers and agents are subject to binding confidentiality obligations; or
- To the professional advisors of either party, provided that such advisors are obligated to maintain the confidentiality of the information they receive.

#### 4.2. Handling the State’s Data

The Contractor must use due diligence to ensure computer and telecommunications systems and services involved in storing, using, or transmitting State Data are secure and to protect that data from unauthorized disclosure, modification, or destruction. “State Data” includes all data and information created by, created for, or related to the activities of the State and any information from, to, or related to all persons that conduct business or personal activities with the State. To accomplish this, the Contractor must adhere to the following principles:

- Apply appropriate risk management techniques to balance the need for security measures against the sensitivity of the State Data.
- Ensure that its internal security policies, plans, and procedures address the basic security elements of confidentiality, integrity, and availability.
- Maintain plans and policies that include methods to protect against security and integrity threats and vulnerabilities, as well as detect and respond to those threats and vulnerabilities.
- Maintain appropriate identification and authentication processes for information systems and services associated with State Data.
- Maintain appropriate access control and authorization policies, plans, and procedures to protect system assets and other information resources associated with State Data.
- Implement and manage security audit logging on information systems, including computers and network devices.

### 4.3. Contractor Access to State Networks Systems and Data

The Contractor must maintain a robust boundary security capacity that incorporates generally recognized system hardening techniques. This includes determining which ports and services are required to support access to systems that hold State Data, limiting access to only these points, and disable all others.

To do this, the Contractor must:

- Use assets and techniques such as properly configured firewalls, a demilitarized zone for handling public traffic, host-to-host management, Internet protocol specification for source and destination, strong authentication, encryption, packet filtering, activity logging, and implementation of system security fixes and patches as they become available.
- Use two-factor authentication to limit access to systems that contain particularly sensitive State Data, such as personally identifiable data.
- Assume all State Data and information is both confidential and critical for State operations, and the Contractor's security policies, plans, and procedure for the handling, storage, backup, access, and, if appropriate, destruction of that data must be commensurate to this level of sensitivity unless the State instructs the Contractor otherwise in writing.
- Employ appropriate intrusion and attack prevention and detection capabilities. Those capabilities must track unauthorized access and attempts to access the State's Data, as well as attacks on the Contractor's infrastructure associated with the State's data. Further, the Contractor must monitor and appropriately address information from its system tools used to prevent and detect unauthorized access to and attacks on the infrastructure associated with the State's Data.
- Use appropriate measures to ensure that State Data is secure before transferring control of any systems or media on which State Data is stored. The method of securing the State Data must be appropriate to the situation and may include erasure, destruction, or encryption of the State Data before transfer of control. The transfer of any such system or media must be reasonably necessary for the performance of the Contractor's obligations under this Contract.
- Have a business continuity plan in place that the Contractor tests and updates at least annually. The plan must address procedures for response to emergencies and other business interruptions. Part of the plan must address backing up and storing data at a location sufficiently remote from the facilities at which the Contractor maintains the State's Data in case of loss of that data at the primary site. The plan also must address the rapid restoration, relocation, or replacement of resources associated with the State's Data in the case of a disaster or other business interruption. The Contractor's business continuity plan must address short- and long-term restoration, relocation, or replacement of resources that will ensure the smooth continuation of operations related to the State's Data. Such resources may include, among others, communications, supplies, transportation, space, power and environmental controls, documentation, people, data, software, and hardware. The Contractor also must provide for reviewing, testing, and adjusting the plan on an annual basis.
- Not allow the State's Data to be loaded onto portable computing devices or portable storage components or media unless necessary to perform its obligations under this Contract properly. Even then, the Contractor may permit such only if adequate security measures are in place to ensure the integrity and

security of the State Data. Those measures must include a policy on physical security for such devices to minimize the risks of theft and unauthorized access that includes a prohibition against viewing sensitive or confidential data in public or common areas.

- Ensure that portable computing devices must have anti-virus software, personal firewalls, and system password protection. In addition, the State's Data must be encrypted when stored on any portable computing or storage device or media or when transmitted from them across any data network.
- Maintain an accurate inventory of all such devices and the individuals to whom they are assigned.

#### **4.4. Portable Devices, Data Transfer and Media**

Any encryption requirement identified in this Supplement means encryption that complies with National Institute of Standards Federal Information Processing Standard 140-2 as demonstrated by a valid FIPS certificate number. Any sensitive State Data transmitted over a network, or taken off site via removable media must be encrypted pursuant to the State's Data encryption standard ITS-SEC-01 Data Encryption and Cryptography.

The Contractor must have reporting requirements for lost or stolen portable computing devices authorized for use with State Data and must report any loss or theft of such to the State in writing as quickly as reasonably possible. The Contractor also must maintain an incident response capability for all security breaches involving State Data whether involving mobile devices or media or not. The Contractor must detail this capability in a written policy that defines procedures for how the Contractor will detect, evaluate, and respond to adverse events that may indicate a breach or attempt to attack or access State Data or the infrastructure associated with State Data.

To the extent the State requires the Contractor to adhere to specific processes or procedures in addition to those set forth above in order for the Contractor to comply with the managed services principles enumerated herein, those processes or procedures are set forth in this agreement.

#### **4.5. Limited Use; Survival of Obligations.**

Contractor may use PI/SSI only as necessary for Contractor's performance under or pursuant to rights granted in this Agreement and for no other purpose. Contractor's limited right to use PI/SSI expires upon conclusion, non-renewal or termination of this Agreement for any reason. Contractor's obligations of confidentiality and non-disclosure survive termination or expiration for any reason of this Agreement.

#### **4.6. Disposal of PI/SSI.**

Upon expiration of Contractor's limited right to use PI/SSI, Contractor must return all physical embodiments to the State or, with the State's permission; Contractor may destroy PI/SSI. Upon the State's request, Contractor shall provide written certification to the State that Contractor has returned, or destroyed, all such PI/SSI in Contractor's possession.

#### **4.7. Remedies**

If Contractor or any of its representatives or agents breaches the covenants set forth in these provisions, irreparable injury may result to the State or third parties entrusting PI/SSI to the State. Therefore, the State's remedies at law may be inadequate and the State shall be entitled to seek an injunction to restrain any continuing breach. Notwithstanding any limitation on Contractor's liability, the State shall further be entitled to any other rights or remedies that it may have in law or in equity.

#### **4.8. Prohibition on Off-Shore and Unapproved Access**

The Contractor shall comply in all respects with U.S. statutes, regulations, and administrative requirements regarding its relationships with non-U.S. governmental and quasi-governmental entities including, but not limited to the export control regulations of the International Traffic in Arms Regulations ("ITAR") and the Export

Administration Act (“EAA”); the anti-boycott and embargo regulations and guidelines issued under the EAA, and the regulations of the U.S. Department of the Treasury, Office of Foreign Assets Control, HIPPA Privacy Rules and other conventions as described and required in this Supplement.

The Contractor will provide resources for the work described herein with natural persons who are lawful permanent residents as defined in 8 U.S.C. 1101 (a)(20) or who are protected individuals as defined by 8 U.S.C. 1324b(a)(3). It also means any corporation, business association, partnership, society, trust, or any other entity, organization or group that is incorporated to do business in the U.S. It also includes any governmental (federal, state, local), entity.

**The State specifically excludes sending, taking or making available remotely (directly or indirectly), any State information including data, software, code, intellectual property, designs and specifications, system logs, system data, personal or identifying information and related materials out of the United States in any manner,** except by mere travel outside of the U.S. by a person whose personal knowledge includes technical data; or transferring registration, control, or ownership to a foreign person, whether in the U.S. or abroad, or disclosing (including oral or visual disclosure) or transferring in the United States any State article to an embassy, any agency or subdivision of a foreign government (e.g., diplomatic missions); or disclosing (including oral or visual disclosure) or transferring data to a foreign person, whether in the U.S. or abroad.

It is the responsibility of all individuals working at the State to understand and comply with the policy set forth in this document as it pertains to end-use export controls regarding State restricted information.

Where the Contractor is handling confidential employee or citizen data associated with Human Resources data, the Contractor will comply with data handling privacy requirements associated with HIPAA and as further defined by The United States Department of Health and Human Services Privacy Requirements and outlined in <http://www.hhs.gov/ocr/privacysummary.pdf>

It is the responsibility of all Contractor individuals working at the State to understand and comply with the policy set forth in this document as it pertains to end-use export controls regarding State restricted information.

Where the Contractor is handling confidential or sensitive State, employee, citizen or Ohio Business data associated with State data, the Contractor will comply with data handling privacy requirements associated with the data HIPAA and as further defined by The United States Department of Health and Human Services Privacy Requirements and outlined in <http://www.hhs.gov/ocr/privacysummary.pdf>.

#### **4.9. Background Check of Contractor Personnel**

Contractor agrees that (1) it will conduct 3<sup>rd</sup> party criminal background checks on Contractor personnel who will perform Sensitive Services (as defined below), and (2) no Ineligible Personnel will perform Sensitive Services under this Agreement. “Ineligible Personnel” means any person who (a) has been convicted at any time of any criminal offense involving dishonesty, a breach of trust, or money laundering, or who has entered into a pre-trial diversion or similar program in connection with a prosecution for such offense, (b) is named by the Office of Foreign Asset Control (OFAC) as a Specially Designated National, or (b) has been convicted of a felony.

“Sensitive Services” means those services that (i) require access to Customer/Consumer Information, (ii) relate to the State’s computer networks, information systems, databases or secure facilities under circumstances that would permit modifications to such systems, or (iii) involve unsupervised access to secure facilities (“Sensitive Services”).

Upon request, Contractor will provide written evidence that all of Contractor’s personnel providing Sensitive Services have undergone a criminal background check and are eligible to provide Sensitive Services. In the event that Contractor does not comply with the terms of this section, the State may, in its sole and absolute discretion, terminate this Contract immediately without further liability.

#### **4.10. Federal Tax Information**

#### 4.10.1. Performance

In performance of this Contract, the Contractor agrees to comply with and assume responsibility for compliance by his or her employees with the following requirements:

1. All work will be done under the supervision of the Contractor or the Contractor's employees.
2. Any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this Contract. Information contained in such material will be treated as confidential and will not be divulged or made known in any manner to any person except as may be necessary in the performance of this Contract.  
Disclosure to anyone other than an officer or employee of the Contractor will be prohibited.
3. All returns and return information will be accounted for upon receipt and properly stored before, during, and after processing. In addition, all related output will be given the same level of protection as required for the source material.
4. The Contractor certifies that the data processed during the performance of this Contract will be completely purged from all data storage components of his or her computer facility, and no output will be retained by the Contractor at the time the work is completed. If immediate purging of all data storage components is not possible, the Contractor certifies that any IRS data remaining in any storage component will be safeguarded to prevent unauthorized disclosures.
5. Any spoilage or any intermediate hard copy printout that may result during the processing of IRS data will be given to the agency or his or her designee. When this is not possible, the Contractor will be responsible for the destruction of the spoilage or any intermediate hard copy printouts, and will provide the agency or his or her designee with a statement containing the date of destruction, description of material destroyed, and the method used.
6. All computer systems receiving, processing, storing, or transmitting Federal Tax Information must meet the requirements defined in IRS Publication 1075. To meet functional and assurance requirements, the security features of the environment must provide for the managerial, operations, and technical controls. All security features must be available and activated to protect against unauthorized use of and access to Federal Tax Information.
7. No work involving Federal Tax Information furnished under this Contract will be subcontracted without prior written approval of the IRS.
8. The Contractor will maintain a list of employees authorized access. Such list will be provided to the agency and, upon request, to the IRS reviewing office.
9. The agency will have the right to void the Contract if the Contractor fails to provide the safeguards described above.

#### 4.10.2. Criminal/Civil Sanctions

1. Each officer or employee of any person to whom returns or return information is or may be disclosed will be notified in writing by such person that returns or return information disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any such returns or return information for a purpose or to an extent unauthorized herein constitutes a felony punishable upon conviction by a fine of as much as \$5,000 or imprisonment for as long as 5 years, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized further disclosure of returns or return information may also result in an award of civil damages against the officer or employee in an amount not less than \$1,000 with respect to each instance of unauthorized disclosure. These penalties are prescribed by IRCs 7213 and 7431 and set forth at 26 CFR 301.6103(n)-1.
2. Each officer or employee of any person to whom returns or return information is or may be disclosed shall be notified in writing by such person that any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this Contract. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of the Contract. Inspection by or disclosure to anyone without an official need-to-know constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as \$1,000 or imprisonment for as long as 1 year, or both, together with the costs of

prosecution. Such person shall also notify each such officer and employee that any such unauthorized inspection or disclosure of the officer or employee (United States for Federal employees) in an amount equal to the sum of the greater of \$1,000 for each act of unauthorized inspection or disclosure with respect to which such defendant is found liable or the sum of the actual damages sustained by the plaintiff as a result of such unauthorized inspection or disclosure plus in the case of a willful inspection or disclosure which is the result of gross negligence, punitive damages, plus the costs of the action. These penalties are prescribed by IRC 7213A and 7431.

3. Additionally, it is incumbent upon the Contractor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a(i)(1), which is made applicable to contractors by 5 U.S.C. 552a(m)(1), provides that any officer or employee of a contractor, who by virtue of his/her employment or official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than \$5,000.

### **4.10.3. Criminal/Civil Sanctions**

The IRS and the Agency shall have the right to send its officers and employees into the offices and plants of the Contractor for inspection of the facilities and operations provided for the performance of any work under this Contract. On the basis of such inspection, specific measures may be required in cases where the contractor is found to be noncompliant with Contract safeguards

## **5. Contractor Responsibilities Related to Reporting of Concerns, Issues and Security/Privacy Issues**

### **5.1. General**

If over the course of the agreement a security or privacy issue arises, whether detected by the State, a State auditor or the Contractor, that was not existing within an in-scope environment or service prior to the commencement of any Contracted service associated with this agreement, the Contractor must:

- notify the State of the issue or acknowledge receipt of the issue within two (2) hours;
- within forty-eight (48) hours from the initial detection or communication of the issue from the State, present an potential exposure or issue assessment document to the State Account Representative and the State Chief Information Security Officer with a high level assessment as to resolution actions and a plan;
- within four (4) calendar days, and upon direction from the State, implement to the extent commercially reasonable measures to minimize the State's exposure to security or privacy until such time as the issue is resolved; and
- upon approval from the State implement a permanent repair to the identified issue at the Contractor's cost; and

### **5.2. Actual or Attempted Access or Disclosure**

If the Contractor determines that there is any actual, attempted or suspected theft of, accidental disclosure of, loss of, or inability to account for any PI/SSI by Contractor or any of its subcontractors (collectively "Disclosure") and/or any unauthorized intrusions into Contractor's or any of its subcontractor's facilities or secure systems (collectively "Intrusion"), Contractor must immediately:

- Notify the State within two (2) hours of the Contractor becoming aware of the unauthorized Disclosure or Intrusion;
- Investigate and determine if an Intrusion and/or Disclosure has occurred;
- Fully cooperate with the State in estimating the effect of the Disclosure or Intrusion's effect on the State and fully cooperate to mitigate the consequences of the Disclosure or Intrusion;

- Specify corrective action to be taken; and
- Take corrective action to prevent further Disclosure and/or Intrusion.

### 5.3. Unapproved Disclosures and Intrusions: Contractor Responsibilities

Contractor must, as soon as is reasonably practicable, make a report to the State including details of the Disclosure and/or Intrusion and the corrective action Contractor has taken to prevent further Disclosure and/or Intrusion. Contractor must, in the case of a Disclosure cooperate fully with the State to notify the effected persons as to the fact of and the circumstances of the Disclosure of the PI/SSI. Additionally, Contractor must cooperate fully with all government regulatory agencies and/or law enforcement agencies having jurisdiction to investigate a Disclosure and/or any known or suspected criminal activity.

- Where the Contractor identifies a potential issue in maintaining an “as provided” State infrastructure element with the more stringent of an Agency level security policy (which may be Federally mandated or otherwise required by law), identifying to Agencies the nature of the issue, and if possible, potential remedies for consideration by the State agency.
- If over the course of delivering services to the State under this Statement of Work for in-scope environments the Contractor becomes aware of an issue, or a potential issue that was not detected by security and privacy teams the Contractor is to notify the State within two (2) hour. This notification shall not minimize the more stringent Service Level Agreements pertaining to security scans and breaches contained herein, which due to the nature of an active breach shall take precedence over this notification. Dependent on the nature of the issue the State may elect to contract with the Contractor under mutually agreeable terms for those specific resolution services at that time or elect to address the issue independent of the Contractor.

### 5.4. Security Breach Reporting and Indemnification Requirements

- In case of an actual security breach that may have compromised State Data, the Contractor must notify the State in writing of the breach within two (2) hours of the Contractor becoming aware of the breach and fully cooperate with the State to mitigate the consequences of such a breach. This includes any use or disclosure of the State data that is inconsistent with the terms of this Contract and of which the Contractor becomes aware, including but not limited to, any discovery of a use or disclosure that is not consistent with this Contract by an employee, agent, or subcontractor of the Contractor.
- The Contractor must give the State full access to the details of the breach and assist the State in making any notifications to potentially affected people and organizations that the State deems are necessary or appropriate. The Contractor must document all such incidents, including its response to them, and make that documentation available to the State on request.
- In addition to any other liability under this Contract related to the Contractor’s improper disclosure of State data, and regardless of any limitation on liability of any kind in this Contract, the Contractor will be responsible for acquiring one year’s identity theft protection service on behalf of any individual or entity whose personally identifiable information is compromised while it is in the Contractor’s possession. Such identity theft protection must provide coverage from all three major credit reporting agencies and provide immediate notice through phone or email of attempts to access the individuals’ credit history through those services.

## 6. Security Review Services

As part of a regular Security Review process, the Contractor will include the following reporting and services to the State:

### 6.1. Hardware and Software Assets

The Contractor will support the State in defining and producing specific reports for both hardware and software assets. At a minimum this should include:

- Deviations to hardware baseline
- Inventory of information types by hardware device
- Software inventory against licenses (State purchased)
- Software versions and then scans of versions against patches distributed and applied

## 6.2. Security Standards by Device and Access Type

The Contractor will:

- Document security standards by device type and execute regular scans against these standards to produce exception reports
- Document and implement a process for deviation from State standards

## 6.3. Boundary Defenses

The Contractor will:

- Work with the State to support the denial of communications to/from known malicious IP addresses\*
- Ensure that the OAKS network architecture separates internal systems from DMZ and extranet systems
- Require remote login access to use two-factor authentication
- Support the State's monitoring and management of devices remotely logging into internal network
- Support the State in the configuration firewall session tracking mechanisms for addresses that access OAKS

## 6.4. Audit Log Reviews

The Contractor will:

- Work with the State to review and validate audit log settings for hardware and software
- Ensure that all OAKS systems and environments have adequate space to store logs
- Work with the State to devise and implement profiles of common events from given systems to both reduce false positives and rapidly identify active access
- Provide requirements to the State to configure operating systems to log access control events
- Design and execute bi-weekly reports to identify anomalies in system logs
- Ensure logs are written to write-only devices for all servers or a dedicated server managed by another group.

## 6.5. Application Software Security

The Contractor will:

- Perform configuration review of operating system, application and database settings
- Ensure software development personnel receive training in writing secure code

## 6.6. System Administrator Access

The Contractor will

- Inventory all administrative passwords (application, database and operating system level)
- Implement policies to change default passwords in accordance with State policies, particular following any transfer or termination of personnel (State, existing MSV or Contractor)
- Configure administrative accounts to require regular password changes

- Ensure service level accounts have cryptographically strong passwords
- Store passwords in a hashed or encrypted format
- Ensure administrative accounts are used only for administrative activities
- Implement focused auditing of administrative privileged functions
- Configure systems to log entry and alert when administrative accounts are modified
- Segregate administrator accounts based on defined roles

## 6.7. Account Access Privileges

The Contractor will:

- Review and disable accounts not associated with a business process
- Create daily report that includes locked out accounts, disabled accounts, etc.
- Implement process for revoking system access
- Automatically log off users after a standard period of inactivity
- Monitor account usage to determine dormant accounts
- Monitor access attempts to deactivated accounts through audit logging
- Profile typical account usage and implement or maintain profiles to ensure that Security profiles are implemented correctly and consistently

## 6.8. Additional Controls and Responsibilities

The Contractor will meet with the State no less frequently than annually to:

- Review, Update and Conduct Security training for personnel, based on roles
- Review the adequacy of physical and environmental controls
- Verify the encryption of sensitive data in transit
- Review access control to information based on established roles and access profiles
- Update and review system administration documentation
- Update and review system maintenance policies
- Update and Review system and integrity policies
- Revised and Implement updates to the OAKS security program plan
- Update and Implement Risk Assessment Policies and procedures
- Update and implement incident response procedures