

# Supplement 1:

**TrustOhio:** Enterprise Security as a Service  
Threat Defense & Monitoring Services

## Table of Contents

1.0	Security as a Service – Trust Ohio: Statewide Foundational Elements	3
1.1	State of Ohio Computing Center (SOCC)	3
1.2	Ohio One Network and OARnet	3
<b>2.0</b>	<b>Establishment of a Statewide Security as a Service (SaaS) Capability: Trust Ohio</b>	<b>4</b>
2.1	Trust Ohio: Overview and General Scope	4
2.2	Proof of Concept Business Objectives and State Requirements	4
2.3	Proof of Concept: Solution Scope Requirements	5
2.4	Proof of Concept Phase Critical Delivery Elements	6
2.5	Location of Services	6
2.6	Contractor Deliverables	6
2.7	State of Ohio Responsibilities	8
<b>3.0</b>	<b>Advanced Security Analytics, Insights and Alerts</b>	<b>9</b>
3.1	Programmatic Security Access Detection and Analytics	10
3.2	Identifying and Remanding Fraudulent, Inappropriate or Suspicious Access Attempts and Other Methods	10
3.3	Integration with Enterprise Security, Notification and Tracking Services	11
3.3.1	General Identification and Integration Requirements	11
3.3.2	State Enterprise Security Event Management System Integration	12
3.3.3	Other Notification Capabilities	12
3.4	Auditing and Reporting Requirements	13
<b>4.0</b>	<b>Enterprise Architecture and Integration Standards and Conventions</b>	<b>13</b>
4.1	Design, Integration and Scalability Considerations	13
4.2	Technical Standards Requirements	13
4.3	Audit and Logging Requirements	14
<b>5.0</b>	<b>Post Proof of Concept Technical, Deployment and Integration Services</b>	<b>14</b>
5.1	Post Proof of Concept Activities: Development of Extensible State Enterprise Standards	15
5.2	Technical, Operations, Change and Scalability	16
5.2.1	General Technical Requirements	16
5.2.2	Performance and Scalability Requirements	16
5.2.3	Operations, Maintenance and Change Management	17
5.3	Security as a Service: Authentication and Access Logging and Reporting	17
5.3.1	Authentication/Access Reporting and Logging	17
5.3.2	System Operational Reporting, Alerts and Notifications	17
<b>6.0</b>	<b>State Project Delivery, Management, Methodology and Approach Requirements</b>	<b>18</b>
6.1	Project Management and Coordination Services	19
6.2	Create and Maintain Project Plan	20
6.3	Project Review Check Point.	21
6.4	Meeting Attendance and Reporting Requirements.	22
6.5	Utilize OIT's Document Sharing/Collaboration Capability	22
6.6	Production/Version Control and Release Management	23
6.7	Maintaining Solution and Operations Documentation	24
6.8	Project Delivery, Role and Responsibility Requirements	24
6.9	System/Environment Administration Support of the Project	25
6.10	Establish and Manage a Program Management & Master Release Calendar	25
6.11	Cooperation with State and State Contractors	25
6.12	Requirements Confirmation and Analysis (for each Proof of Concept)	25
6.13	Analyze Phase Requirements	25
6.14	Design Phase Requirements	26
6.15	Build Phase Requirements	26
6.16	Test Phase Requirements	27
6.17	Deploy Phase Requirements	28
6.18	Knowledge Transfer and Production Handoff	30
6.19	Project Completion Activities, Final Documentation and Post Implementation Support Obligations	30
6.20	Future Project Services Pricing Response and Rate Card	31
<b>7.0</b>	<b>Schedule of Deliverables and Work Products</b>	<b>31</b>
7.1	Delivery and Deliverable Standards	31
7.2	Schedule of Key Project Management Work Products	31
<b>8.0</b>	<b>Assumptions</b>	<b>34</b>
8.1	Support Requirements	34
8.2	Pre-Existing Materials	35
8.3	Commercial Materials	35

<b>9.0</b>	<b>State Staffing Requirements</b>	<b>35</b>
9.1	Contract Staffing and Key Activities	36
9.2	Staffing Plan and Time Commitment	37
<b>10.0</b>	<b>Service Level Requirements: Security as a Service</b>	<b>38</b>
10.1	Service Level Specific Performance Credits	38
10.2	Overall Contract Performance	39
10.3	Monthly Service Level Report	40
10.4	Service Availability	40
10.5	Priority 1 Outage Resolution Time	40
10.6	Service Level Specific Performance Credits	41
<b>11.0</b>	<b>Service Level Requirements: State Systems Integration Projects</b>	<b>41</b>
11.1	Service Level Specific Performance Credits	41
11.2	Overall Contract Performance	43
11.3	Monthly Service Level Report	43
11.4	Service Level Commitments – Project Implementation Services	43
11.5	Service Level Specifications	45
11.5.1	Defect Resolution – Mean Time to Repair/Resolve (Priority 1 Items)	45
11.5.2	Defect Resolution – Mean Time to Repair/Resolve (Priority 2 Items)	46
11.5.3	Defect Resolution – Mean Time to Repair/Resolve (Priority 3 Items)	47
11.5.4	Service Levels – Testing Performance	48
11.5.5	Blocking Issues – Identification and Removal	49
11.5.6	Regression Testing Performance – Issue Find/Fix Rate	50
11.5.7	Code Coverage – Automated Test Beds	51
11.5.8	Service Levels – Project Performance	52
11.5.9	Issue Reporting	53
11.5.10	Deliverable Acceptance	54
11.5.11	Support of State User Acceptance Testing Activities	55
11.5.12	Service Levels – Development Methodology Compliance	56
11.5.13	Service Levels–Project Delivery–Build/Test Activities as a Percentage of Overall Activities	57
11.5.14	Service Levels – Project Completion – Issues Detected and Resolved In Production	58

**Supplement One** contains State requirements for the creation, establishment and operation of a Statewide (State, Federal, K-12 institutions, Higher Education, Municipal/Local County Government and Cooperative Purchasing Partners) Security as a Service inclusive of the Service itself, implementation of a State of Ohio fully production operational Proof of Concept and the implementation of programmatic analytics to identify and significantly reduce the State’s exposure and response times to threats. A **single Contractor** may be awarded this Work, based upon the State’s evaluation of proposals for Supplement 1.

## 1.0 Security as a Service – Trust Ohio: Statewide Foundational Elements

The State maintains two significant assets to serve as the foundation for this effort: The State of Ohio Computing Center (SOCC) and the Ohio One Network / OARnet. As an overview:



Beyond providing a nationally recognized statewide infrastructure, OARnet specializes in providing custom solutions to fit clients' individual needs, whether promoting efficiencies and shared services throughout Ohio's public institutions, providing worldwide connectivity through Internet2 tie-ins, bridging dozens of international sites with high-definition telepresence or supplying engineering solutions via the 24/7 Network Operations Center.

### 1.1 State of Ohio Computing Center (SOCC)

#### Facility

- The SOCC is considered one of the largest computer facilities in the country with more than 360,000 square feet of total space, 220,000 of which is capable of supporting mission critical computing
- The SOCC is conveniently located on the campus of The Ohio State University, making access and usage easy from a commuting, logistics and practical perspective.
- The SOCC is a Tier III capable facility with several Tier IV features. Power, cooling and telecommunications are fully redundant and supported by onsite UPS and Diesel power generation. The SOCC has been continuously operational for more than 20 years.

#### Capabilities

- The SOCC is a peer on the OARnet network, as such we have effectively unlimited access to OARnet bandwidth. The OARnet point(s) of presence are distributed throughout the facility.
- Federal, K-12 institutions, Higher Education, Municipal/Local County Government and Cooperative Purchasing Partners computing locations are separate and distinct from State computing functions within the facility. As such, these users can access, upgrade and operate in a private and secure suite in the SOCC, separated physically and logically within the facility from a floor, bay, rack and network perspective.
- The facility has ample power and cooling to exceed State requirements today and for the foreseeable future. Following the completion of our remediation effort in 2014, effectively doubled the power available to all SOCC customers.

### 1.2 Ohio One Network and OARnet

The State's Ohio Academic Research Network (OARnet) is the envy of many Public Sector entities – both State and Federal alike – and due to its ultra-high bandwidth (100 gigabit) and Statewide pervasiveness we are in a most fortunate position with regard to networking.

Through Ohio One Network, the State is leveraging OARnet and consolidating its networking needs across all of our Agencies, computing concentrations and locations as a centrally administered and managed network that connects more than 100 State Agency, Board and Commission locations: administrative, computing, or otherwise.

Agencies who leverage OARnet at the closest point of presence (PoP) access the State backbone, the State's Private Cloud, Agency systems contained in the SOCC as well as Enterprise Services such as Office365, Document Management, Collaboration tools and the like. Via the Ohio One network, Agencies can now compute, collaborate and better serve our citizens.

In addition, State Higher Education Institutions are leveraging OARnet to migrate their production and disaster recovery functions to the State Data Center (SOCC), realizing IT savings in a similar fashion to what the State is enjoying through consolidation of IT infrastructure and operations.

## **2.0 Establishment of a Statewide Security as a Service (SaaS) Capability: Trust Ohio**

### **2.1 Trust Ohio: Overview and General Scope**

The State of Ohio is seeking a production deployment of a proof of concept (live use, limited scope) to be provided by a qualified Contractor to perform Security Systems Integrator (SSI) services to establish the Statewide Security as a Service inclusive of tools, tool integration with the State SIEM, operating methods and procedures, and IT Security Policy input for deployment to the State Enterprise (collectively more than 120 Agencies, Boards and Commissions). This effort is named “**Trust Ohio**” and must be designed and implemented to determine the feasibility of using managed security services to:

- Enhance the detection of cyber threats affecting entities within the State of Ohio;
- Provide cyber intelligence to the State in order to increase cybersecurity defenses and information sharing with various government, education, and business organizations; and
- Assist the State in response to cybersecurity events and incidents.

The proof of concept must be extensible in future phases to also test the delivery of security services to State, Federal, K-12 institutions, Higher Education, Municipal/Local County Government and Cooperative Purchasing Partners to validate that the services are applicable to these types of organizations.

The “Trust Ohio” Proof of Concept (POC) will be a limited scope, full production implementation of the State's planned “Trust Ohio” security service. The purpose of the POC is to provide evidence that the proposed services can provide the intended benefits to the State of Ohio.

### **2.2 Proof of Concept Business Objectives and State Requirements**

The States requirements are a working Service inclusive of the design, implementation and production (i.e., Live Commercial Use) solution are (by Area). The Contractor must:

#### **Security Profile Enhancement and Service Design**

- Determine the need for decryption or packet inspection services as part of performing the inspection of network traffic.
- Determine existence of specific privacy issues that may impact the security services
- Confirm traffic separation is maintained among any participating entities.

- Determine the need and interest level for each security service and develop a tiered service model that can be used by State, Federal, K-12 institutions, Higher Education, Municipal/Local County Government and Cooperative Purchasing Partners, and potentially the business community for future production services
- Confirm the level of services appropriate for each type of participating entity

### **Security Threat Identification**

- Provide proactive identification of all cyber risks and attacks including ones that the State of Ohio has previously not been able to detect.
- Validate the integration of all technology components and end-to-end data flow/incident management processes

### **Establishment of Operating Procedures, Protocols and Coordination/Communication Mechanisms**

- Ensure communication and resolution of identified security threats.
- Develop close integration and information sharing with State and Federal Threat Intelligence Agencies via the Ohio Homeland Security Strategic Information and Analysis Center
- Develop and validate a governance model for the services
- Create an efficient method for onboarding future participating entities

### **Operation, Monitoring and Reporting**

- Provide 24x7 cyber threat intelligence and monitoring services
- Provide weekly threat and incident reports to the State
- Validate volume of network traffic
- Confirm there is no degradation of Internet traffic to and from the State of Ohio as a result of the services.
- Outline Higher Education Cooperatives, internship programs, and Ohio Science, Technology, Engineering and Mathematics (STEM) opportunities for cyber workforce development.
- Define and implement requirements for the development of an Ohio Cyber Security Threat Map that can be updated near real-time by the service provider to indicate threats affecting or originating from Ohio entities
- Confirm the ability to selectively parse traffic to optional services in order to provide extended security services to specific network traffic types

## **2.3 Proof of Concept: Solution Scope Requirements**

To accomplish the scope requirements, the Contractor, must provide appropriate equipment (to be located at the State of Ohio Computer Center (SOCC) implementation and management of the following services as part of the production POC. The technical scope of the POC must include the following:

- Firewall/Intrusion Detection/Intrusion Prevention Protection
- Advanced Malware Protection
- Security Event Identification and Alerting Services
- Web Security Services
- Security Data Analytics
- Distributed Denial of Service Protection Services
- Data Loss Prevention Monitoring Services

The Contractor will:

Establish a definitive set of functional and technical requirements for the technical scope of service and design and implement all elements required for operation in a production environment inclusive of the following:

- Hardware and Network Appliances
- Network Software and Monitoring Tool Software
- Analytics and Correlation Software and Tools
- Operational Processes and Procedures
- State Network Team Change Management and Training
- Participating Agency Change Management and Training
- Network Monitoring and Alerting Tools and Tool Integration with the State SIEM
- Other equipment, Tools, Processes required to satisfy the State's business, functional and technical requirements contained in this Supplement.

## 2.4 Proof of Concept Phase Critical Delivery Elements

The Contractor must provide the following delivery elements:

- Project Plan, Staffing Plan and Other Project Delivery Requirements as further specified in this Supplement in its totality;
- Requirements Gathering, Design and Implementation to Production of the Proof-of-Concept;
- Implementation of all required hardware, software, integration and reporting/dashboard requirements as mutually agreed;
- Service Operation Documentation inclusive of Processes, Procedures, Roles/Responsibilities and Other elements as required to operate the Security as a Service Solution in the State's production environment;
- Documented Use Cases and Results;
- Development of a Business Case for Ongoing Investment, Operation & Maintenance and Deployment(s) at the State's request beyond the Proof of Concept for a mutually agreeable Scope under a State Authorized Statement of Work or IDA as applicable;
- Draft plan for the deployment and operation of "Trust Ohio" for State identified user constituencies as future phases including State, Federal, K-12 institutions, Higher Education, Municipal/Local County Government and Cooperative Purchasing Partners.

As part of delivering the work, the Contractor will identify all opportunities for State security personnel to participate in, operate and collaborate with the overall Service (as a whole) as well as any service delivery elements (e.g., software, hardware, appliances and the like) as to increase the State's overall capability to understand and participate in the operation of the Solution as an active participant.

## 2.5 Location of Services

Services are to be performed at a combination of sites which must include the State of Ohio Computer Center and may include other facilities within the United States. **All services and data must remain within the United States. Offshore access to any element of the Solution, Service, State specific deliverables, work products, technical details or other data is not permissible under any circumstances.** All work is subject to Executive Order 2011-12K as contained in the RFP Documents.

## 2.6 Contractor Deliverables

As part of the work, the Contractor will:

- Deliverable 001.** Perform a baseline assessment of the environment, focusing on logging, network services, and vulnerabilities.
- Obtain Netflow flows from network devices for analysis by Cisco's Data Capture & Analysis POD (DCAP)
  - Incorporate each asset associated with the Cisco backend infrastructure Network devices, that are located within the SOCC, that have been identified, classified, and prioritized in the previous stage as part of ongoing active scanning from the DCAP to determine open/listening network services (ports).
- Deliverable 002.** Perform active scanning to attempt to enumerate the version of the services that are listening. The results of the scans are to be compiled, documented and reviewed with State security personnel.
- Tune data capture and analysis based on State furnished information on normal and permissible traffic flows and identify and (to the extent possible) eliminate all non-permissible flows.
- Deliverable 003.** Assess network traffic via DDoS services and report any traffic that would be prevented in the production release of "Trust Ohio" to demonstrate the validity and completeness of the Solution.
- Deliverable 004.** As identified by the State, complete analysis on the State's web traffic using Web Security Services and Data Loss Prevention services. This analysis is to report on incidents that could have been prevented.
- The Contractor is not to block any traffic arising from incidents from occurring unless first authorized by the State of Ohio.
  - A report from these services is to be produced and reviewed with State security personnel on a weekly basis.
- Deliverable 005.** Implement and perform IPS monitoring and reporting on suspicious traffic.
- Deliverable 006.** Integrate threat intelligence feeds with Ohio Homeland Security and U.S. Homeland Security via the State fusion center.
- Deliverable 007.** Define and document the integration of the incident response process used by the State with a proposed State-wide Incident Response and Governance process. This process must address the items below:
- Definition of an incident
  - Communication of incidents to the State Information Security Incident Response Team
  - Location affected (e.g. IP address, subnet, data center, etc.)
  - Assets (e.g. servers, data, network, etc.) affected
  - Determination if the compromised system(s) have been modified
  - Recommended steps to mitigate the incident(s)
  - Recommended steps to remediate the incident(s)
- Deliverable 008.** Conduct a transition briefing with the State at the completion of on-boarding to the service
- Deliverable 009.** Implement a customer portal for the service and provide instructions for its use to be composed of both incident ticket management and security reports (e.g. incident rate of occurrence, daily threat exposure, top 10 sources of attack)
- Deliverable 010.** Implement, validate, operate and maintain DCAP

- Deliverable 011.** Detect, respond to, and remediate security incidents by analyzing network traffic, evaluating security telemetry, and leveraging intelligence feeds including:
- Creation of incident tickets after the Solution or State detects an incident or an in-scope manual submission of an incident by the State.
  - Identification of incidents rated High severity (as mutually defined with the State, generally those that present an active threat) must be communicated to the State within 15 minutes after the incident is confirmed.
  - Identification of Medium severity (as mutually defined with the State, generally those that present a high risk, but not active threat) incidents must be communicated within 1 hour after the incident is confirmed.
  - Coordination of the management of the incident, which includes communicating with the State Information Security Incident Response Team throughout the incident management lifecycle (detection, investigation, mitigation, remediation).
  - Notification to the State that the incident has been resolved or remediated.
- Deliverable 012.** In collaboration with the State, determine a categorization for incidents using the US-CERT guidelines including:
- Communication and Coordination Processes, Procedures and Templates for; State Internal Use; between the State and Local/Municipal Governments; within the Local Government community; between the State and the Education Community; within the Education community; and within the Private Sector if reported to the State.
  - SLAs and ratings based upon these categorizations must be defined and agreed upon during the POC.
  - Standards to Define Severity, Prioritization and Close-out of all incidents.
- Deliverable 013.** Provide a training session to share best practices and review lessons learned from the POC.
- The Contractor will provide a proposal for production services at the end of the POC, customized to State of Ohio requirements and business objectives.
- Deliverable 014.** Creation of a communications presentation (e.g., “Marketing Deck”) designed to highlight the scope, use and usefulness of the overall Solution to build understanding and awareness within the State IT and Security community. This presentation should be suitable for onward communications with peers in Local/Municipal Governments and the Education Community that is designed to foster adoption and implementation of the Service Statewide.
- Deliverable 015.** Certify in writing the destruction of all data on all hard drives and device configuration information that do not remain with the State at the conclusion of the engagement. All data destruction and sanitization of equipment is to be performed using procedures consistent with NIST special publication 800-88. Offeror note: The State maintains a similar capability via a 3<sup>rd</sup> party Contractor that can be utilized upon mutual consent of the State and Contractor.
- Encrypt traffic via VPN during the performance of any remote analysis of security incidents.

## 2.7 State of Ohio Responsibilities

The State will be responsible for the following:

- The State will provide resources and contacts to assist the Contractor in assessing the State’s strategies, environment, and security workflow.
- Key stakeholders will participate in interviews, onboarding processes, and deliverable reviews.

- The State will provide appropriate IP addressing schemas, updated network diagrams, and other technical information needed for the DCAP and initiation of security monitoring by the Contractor. This information must be kept secured in accordance with existing Non-Disclosure Agreements that are maintained with the State of Ohio.
- Appropriate resources will be provided to review the asset classification and prioritization documents and to assist the Contractor with the process of documenting the identification, classification, and prioritization of critical systems and data.
- The State will provide network use descriptions, policies, and other information to provide an understanding of what is normal and permissible network traffic.
- The State will provide response policies, guidelines, and contacts, aligned with local/state/federal law and regulations. The State will define and direct the response and communicate this to the Contractor. The contact list will identify the proper State resources for notification and escalation that have the authority to make decisions and to triage events and identify additional State resources that may be needed.
- The State will define the situations and locations in the network where full packet capture may not be permissible and will provide this information to the Contractor.
- Security representatives will be designated to participate in Contractor project completion briefings or after action reports.
- The Contractor will be notified immediately if an incident is detected by the State. The Contractor will then create a ticket and initiate an investigation
- When, and if appropriate, the State will implement recommended mitigation techniques and perform remediation activities as necessary on affected State assets.
- If the State cannot attend the knowledge transfer sessions it will arrange for the Contractor to provide representation.
- The State is responsible for ensuring the parsing out of the Ohio Public Library Information Network (OPLIN) traffic prior to routing State traffic into the Trust Ohio infrastructure.
- Unless otherwise agreed, the State will respond within three to four business days of the Contractor's request for any other documentation or information needed to provide the service.
- The Contractor will provide collaboration tools for State personnel use for hosted meetings, documentation management, instant messaging, desktop sharing and use of collaborative spaces.
- Subject to successful Contractor (i.e., individual team members) completion of State required Background and applicable Drug testing the State will grant Contractor personnel access to the SOCC and State Networks as required.

### 3.0 Advanced Security Analytics, Insights and Alerts

The State wishes to identify, design, implement and deploy an Enterprise Level Security Analytics, Insights and Alerts detection capability, initially focused on matters complimentary to the scope of this RFP (i.e., Security as a Service), but extensible to other generalized uses in the State's IT applications and infrastructure portfolio. The proposed solution should be complimentary to existing State capabilities including but not expressly limited to network level security and protection of computing assets and facilities as well as Infrastructure Level capabilities including but not limited to centralized intrusion detection, reporting, notifications as well as network level protections around State firewalls, network access/egress points, web servers, load balancers, hardware, servers, networks, storage and the like.

Therefore, Contractor must propose a Service (or framework of systems comprising an overall solution) that addresses all requirements in this Section, and as a result of the work in this Supplement, implement specific

capabilities limited to support the Proof of Concept as defined and required in this Supplement, but extensible and scalable to the needs of the State, extended to Federal, K-12 institutions, Higher Education, Municipal/Local County Government and Cooperative Purchasing Partners that may choose to utilize these aspects of the system.

### 3.1 Programmatic Security Access Detection and Analytics

The Contractor must specify, design, implement and deploy a system to programmatically identify inappropriate access, intrusion, or suspected attempts at access that runs as a real-time background processes (transparent to users) that utilizes all available (both State and External Sources) contextual attributes and data points such as geolocation, device characteristics, user behavior, navigations and transaction activity to determine the likelihood of inappropriate access.

The system will compare this information to expected behavior using machine learning or statistical algorithms, or State defined or Contractor proposed “best practice” rules that define "abnormal" access behavior and activities.

The system will verify legitimacy of a user's attempted access and network use using available internal and external information sources including the comparison of incoming identity information and contextual attributes (as described above), and comparing against available external and internal information (as required).

The Contractor is responsible for the following Deliverables for this section:

**Deliverable 016.** Intrusion Detection/Analytics Requirements Scoping, Elaboration and Confirmation Document

**Deliverable 017.** Intrusion Detection/Analytics Design Document based on Requirements

**Deliverable 018.** Intrusion Detection/Analytics Functional and Technical Build Completion Acceptance

**Deliverable 019.** Intrusion Detection/Analytics System Test Completion Acceptance

**Deliverable 020.** Intrusion Detection/Analytics User Acceptance Testing Completion

**Deliverable 021.** Intrusion Detection/Analytics Deployment to Production

**Deliverable 022.** Intrusion Detection/Analytics Post-Production Completion Activities and Acceptance

### 3.2 Identifying and Remanding Fraudulent, Inappropriate or Suspicious Access Attempts and Other Methods

The Solution must include, and be designed, implemented and deployed to leverage a combination of rule-based (State and Industry Best/Common Practice) methods as well as statistical or machine learning techniques to enable the linkage and relationships across users and other entities and their attributes using multivariate data stores to detect inappropriate access.

The Solution must include, and be designed, implemented and deployed to analyze and correlate network, user and other entity behavior across different access channels, modes and devices, and prioritize alerts and warnings using a combination of State and Best/Common practices, rules and statistical methods.

The Solution must include the capability to be extended to monitor and analyze network, user and entity behavior as well as to identify anomalous or inappropriate network, user or entity behavior using a combination of State and Best/Common practices, rules and statistical methods.

The Solution must be designed, implemented and deployed to:

- Detect account takeover, which can occur when user account credentials are stolen (for example, via malware-based attacks);
- Detect repeated or systemic attempts at password hacking, denials of service (distributed or otherwise) or other means to circumvent, suspend, bypass, breach or render unusable State network and computing assets

inclusive of web, application, database applications as well as network level devices such as firewalls, routers, load balancers and the like;

- Identify and detect automated scripts targeting networks, accounts or an Agency system or infrastructure asset;
- Identify and detect automated scripts engaged in a massive attack against a large number (hundreds and thousands) of network elements, systems, and accounts;
- Identify and detect attributes pertaining to an individual conducting a manual or coordinated attack (e.g., source, IP address(es), country, location and other identifying attributes) to assist the State in both protections from the attack as well as pursuing additional means to reveal the origin/source of the attack;
- Identify and detect a combination of human(s) and automated script(s) executing either targeted or mass attacks; and
- Identify and detect fraudulent or suspicious access via location based, network, device, browser or other methods that are inconsistent with authorized legitimate access.

The Proposed Solution must support user and entity profiling and behavioral analytics, such that a network, user's or entity's ongoing behavior is captured in a profile that can subsequently be used to compare against new activity to determine whether the activity is legitimate.

The Proposed Solution must include anomaly detection capabilities using statistical models, rules, or a combination of both. Ideally, one or more of each type of statistical model must be supported by the Solution for State use.

Solution modeling capabilities must include:

- Confirmed "bad" behavior and access methods that indicate illegitimate access;
- "Normal behavior," most of which is assumed to be "good." Including common system uses, navigation transactions, transaction limits, historical transaction levels and values and other factors;
- The Solution should, as part of routine functions establish a history of confirmed fraud and bona-fide use, and include baselining various activities and entity behaviors;
- Detection of anomalies that deviate from established baselines but include controls to help the State to manage transactions holistically realizing that not all anomalies represent intrusion or attempts to deny service through any means;
- Continuous behavioral profiling of networks, traffic, accounts and entities;
- Ingesting and integrating external threat intelligence into intrusion detection analysis and operations, initially from the State's Enterprise SIEM;
- Using the above data sources and other State data to compare incoming traffic or transactions across online channels with existing profiles and norms of user or entity behavior in order to detect intrusions or denials of service; and
- Establish linkages and correlations between, fraud detection uses rules, statistical models or both and linkages across key attributes, such as device, name, IP, phone, address and email address and other factors, to find patterns of suspect activities.

The Contractor is responsible for the following Deliverable for this section:

**Deliverable 023.** State SIEM Integration Verification

### 3.3 Integration with Enterprise Security, Notification and Tracking Services

#### 3.3.1 General Identification and Integration Requirements

Should the Solution determine that one or more of: 1) a known fraudulent access attempt; 2) apparent fraudulent activity; or 3) suspicious activity or traffic the Contractor's provided Solution must:

- Suspend access to the State, if actual behavior is out of range with what's expected or if the user appears suspect;
- Remand attempted access to the system to the State to conduct further review and investigation of the traffic, transaction or user, as warranted;
- Be configurable to initiate State (or State Agency) specific workflows related to suspending, limiting, blocking or if necessary terminating access inclusive of (at the State request) remanding the access or attempted access to data to State or Federal authorities as determined.

### 3.3.2 State Enterprise Security Event Management System Integration

As part of project initiation activities, the Contractor will conduct requirements and design sessions with the State Security group to establish a definitive set of “**security events**” that are available within the proposed solution elements by area including Offeror Proposed Security as a Service platform or service; capabilities within the scope of Proof of Concept networks and the proposed network analysis, logging and intrusion detection solution.

Given this mutually agreed set of solution events, the Contractor will implement integration between the proposed solution elements and services and the State's SIEM and support the State in the development of security alerts, warnings, programmatic system actions (e.g., suspend network or user access, require re-validation of IDs, alert Agency or State security staff) and other features as required to support the State in identifying intrusive or inappropriate access to State systems so that the State can take action as it requires within the context of State systems, networks, computing platforms and other means as to minimize the State's exposure to intrusive, unapproved or inappropriate access.

The Solution must support real-time replication or integration of audit logs to the State's Security Information and Event Management (SIEM) solution: IBM QRadar® Security Intelligence Platform for audit reporting, alerting and management by State Security and Privacy Personnel.

The Contractor will ensure that non-State related SEIM events, with the exception of those that impact or pose a risk to the State, are not incorporated into all security event feeds to the State's SEIM.

### 3.3.3 Other Notification Capabilities

The proposed Solution must be designed, implemented and deployed to:

- Support electronic notification of high levels of, or programmatic fraud that meet State defined parameters and utilize existing notification protocols and capabilities in the State such as text message, email and other common communications formats; and
- Be extensible to be integrated into operational consoles utilized to protect State physical, logical, virtual, infrastructure and application level Agency users and State responsible parties. By way of an illustrative use case: alert an Agency system or security manager via email that his/her system is under attack or probing via fraudulent access, credentials or other means.

The Contractor is responsible for the following Deliverables for this section:

**Deliverable 024.** Implemented Compendium of Tracked System Events and System Notification Workflows inclusive of:

- State SIEM Integration Design inclusive of all Tracked System Events
- Successful Completion of Contractor System Testing
- Successful Completion of State SIEM System Acceptance Testing

- Final State Acceptance pertaining to Production Deployment

### 3.4 Auditing and Reporting Requirements

The Intrusion/Access Detection and Management solution must:

- Be capable of producing audit reports via either Contractor provided web reporting tools or State access via State standard reporting tools (IBM/Cognos and/or Tableau);
- Have the capability to generate ad-hoc business reports that can support internal State invoicing needs including Agency use/consumption, application level access and proration of the entire Service based on Agency actual use/consumption;
- Be capable of producing a web accessible report dashboard with the ability to export the report in CSV, PDF and Excel as appropriate to the content of the report;
- Not display or maintain sensitive personal or confidential infrastructure information in logs or administrative messages; and
- Be capable of generating a report for a specific customer pseudonymous identifier when the identifier is required to support other functionality.

As part of the work the Contractor will:

- Investigate security incidents and determine root causes and prevention/mitigation actions required to prevent similar issues from reoccurring.
- Make recommendations and work with the State to resolve, restore, and remediate network issues, defects or vulnerabilities as applicable.
- Close incidents upon remediation.
- Manage all technologies, regardless of location including the SOCC and Agency locations that support the Solution infrastructure needed for the service including any in-scope or 3<sup>rd</sup> party vendor products.

## 4.0 Enterprise Architecture and Integration Standards and Conventions

### 4.1 Design, Integration and Scalability Considerations

**General Enterprise User Counts and Sizing Considerations** Contractors are to design and implement the proposed Solution to directly support the sizing required in the Agency Projects specified elsewhere in this Supplement, and be capable from an architectural/sizing perspective, to be scalable to address the following **approximate** populations:

Measure / Sizing Points	Approximate Count
Ohio Population (All Citizens)	11.6M
Ohio Households	4.5M
Ohio Registered Businesses	7.5M
State of Ohio Worker Population	54,000
State of Ohio State, County and Local Government Worker Population	738,000
Agency Systems Inventory (Total)	2,600+
Agency Systems that Maintain some form of sensitive personal or financial information	1,500

### 4.2 Technical Standards Requirements

The proposed Solution must comply with the following technical standards and requirements:

- Provide a secure channel for real time data transmission between State and the proposed Service Provider(s).

- Use standards-based web services technology, including SOAP, WS-Security, and XML.
- Be in compliance with all Federal standards and guidelines, including:
  - OMB M 04-04: E-Authentication Guidance for Federal Agencies;
  - NIST SP 800-63: Identity Proofing at Assurance Level 3;
  - FIPS 140-2: Encryption for backend data verification calls;
  - NIST SP 800-30: Risk Management Guide for Information Technology Systems; and
  - NIST SP 800-95: Secure Web Services for backend data verification calls.

### 4.3 Audit and Logging Requirements

The Solution must provide full and configurable auditing capabilities, including the creation/deletion of users, password resets, role/privilege assignment, token assignments, multi factor method(s) and devices, etc.

System must provide full auditing of access to applications, resources, and individual user accounts.

All auditing logs must be reviewable by state security administrators and security policy staff using access to system logs and via the Programmatic Fraud Detection system(s) proposed by the Contractor.

The Solution must support real-time replication or integration of audit logs to the State's Security Information and Event Management (SIEM) solution IBM QRadar® Security Intelligence Platform for audit reporting, alerting and management by State Security and Privacy Personnel.

The Solution must be configurable for auditing events and be extensible to support situational analysis of events and breeches (active and retrospectively) as to support incorporation of new rules, methods, tools and techniques to further enhance the State's overall security posture in the future.

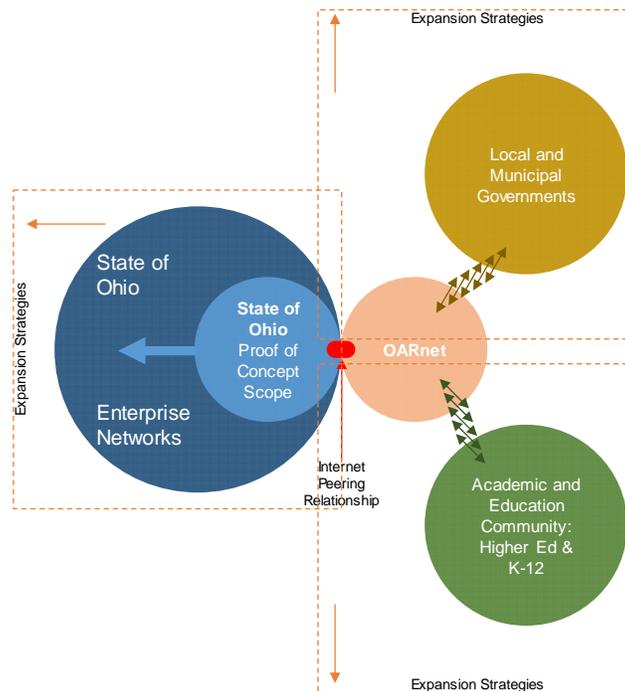
All Solution activity must be attributed and logged to a single, unique system user, identifiable to individual persons.

### 5.0 Post Proof of Concept Technical, Deployment and Integration Services

The State has identified a need across the Enterprise for the services and capabilities contained within this RFP. The following is a conceptual overview of potential deployment of the Services and Capabilities required by this RFP in total, and initially in a live, production use, Proof of Concept and onwards implementation and adoption by State Agencies as an Enterprise Standard based on State established priorities and identified opportunities.

Based on the success of the Proof-of-Concept and its use and effectiveness in Production, the State may elect to not only expand this offering for its own use, but offer Local/Municipal Governments and the Academic/Education constituencies in the State access to the tools, methods, Service and other elements of the Service to enhance their positions with respect to Security and Intrusion detection and prevention.

#### **Conceptual, Proof of Concept and Post Proof of Concept Implementation Approaches**



## 5.1 Post Proof of Concept Activities: Development of Extensible State Enterprise Standards

As part of the conclusion of the Proof of Concept project, the Contractor will develop a set of extensible State Enterprise standards as a deliverable for the specification, use of and standards pertaining to the developed enterprise solution based on the successful completion of the Proof of Concept Project.

**Deliverable 025.** Extensible State Enterprise Standards to include:

- The Security as a Service inclusive of integration, validation, technical, testing and other details pertinent to the State or a capable third party of the State's choosing to incorporate the features, functions and capabilities developed for the initial Proof of Concept for other State Agencies who may wish to incorporate developed capabilities in their systems or services.
- Any and all Enterprise level integrations, configurations, extensions, workflows, conversions and other elements pertinent to the operation, maintenance or extension of Enterprise Security as a Service associated with the aforementioned Services including operation manuals, release notes, test cases and results, technical contacts and documentation as provided or utilized in performing the Work for the initial Proof of Concept.
- Any and all Enterprise level integrations, configurations, extensions, workflows, conversions and other elements pertinent to the operation, maintenance or extension of Intrusion and Fraud Detection elements associated with the aforementioned Services including operation manuals, release notes, test cases and results, technical contacts and documentation as provided or utilized in performing the Work for the initial Proof of Concept.
- During the Project, the Contractor will conduct informal information sharing and knowledge transfer services coincident with the delivery of the Services in this RFP and on a formal basis at the conclusion of the project in such a manner as to ensure that State personnel assigned to support, develop, manage or participate in the operation of the Trust Ohio platform are apprised of the contents of each environment inclusive of features, functions, extensions, 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 services.

- These services shall be designed and delivered in a manner as to provide the State assistance, cooperation and information as is reasonably necessary to help enable a smooth transition of the applicable services from participating Agencies and any Contractors associated with the development, operation or maintenance of the systems contained in the Proof of Concept. 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.

## 5.2 Technical, Operations, Change and Scalability

### 5.2.1 General Technical Requirements

- The Solution must support and be implemented with a failover configuration to ensure high availability. The Solution must not have a single point of failure.
- The Solution must support full back up and restore capabilities so that the Solution (inclusive of software elements, data, configuration value and other elements as required to operate the Solution) can be restored from media with minimal additional intervention.
- The batch and backup operations must not degrade the response times of the system in off hours, assuming a lower request load to be estimated and justified by the Service Provider.
- The Contractor hosted Primary Production and Disaster Recovery sites and all State data must be in the United States and located as to be technically diverse from the primary production site. Technical diversity factors include at a minimum: alternative and redundant power providers or grids, telecommunications network providers to those servicing the primary and disaster recovery sites respectively.
- The Contractor must execute annual DR testing and provide the State with documented results and a remediation plan with committed resolution dates for any item identified as a weakness, material or otherwise from a technical, process, procedural or organizational perspective as provided to the State by the Contractor under this RFP.

### 5.2.2 Performance and Scalability Requirements

Solution must support a minimum of 99.99% uptime for 24 x 7 x 365 operations. (Note: see Service Level Requirements Section for additional specifics).

Solution must support a peak load of twice (2x) the expected maximum concurrency to ensure adequate spare capacity for growth and expansion without an unacceptable degradation of performance.

The Contractor and the State will review actual peak load data no less frequently than twice yearly and mutually make sizing increase and deprecation decisions based on the actual load of the Solution. As this RFP affords, and the State anticipates, additional adoption of Agencies and other Governmental and Education bodies based on State priorities in the future, the Contractor and State will review performance in advance of any such significant onboarding activity in the context of the then current performance and available capacity of the system and make adjustments as appropriate as to maintain a positive user experience from a performance and availability perspective and as to support ongoing attainment of Service Level Requirements.

The Contractor is responsible for the following Deliverable for this section:

**Deliverable 026.** System Performance Test Results (Proof of Concept)

**Deliverable 027.** System Scalability Plan based on Extensibility to the State Enterprise and other State identified User Constituencies (e.g., Local/Municipal Government, Education etc.)

### 5.2.3 Operations, Maintenance and Change Management

The Contractor, via its proposed Solution must provide a regular patching mechanism, consistent with trust zone constraints (no internet access allowable in certain zones).

The State must be notified of any emergency maintenance activities that must be performed on internal or external components. A mutually approved procedure must be established by the State and Contractor.

The Contractor must comply with Ohio Request for Change (RFC) and change control management procedures which will be jointly developed to mutual satisfaction of the parties in the context of the proposed solution, but nonetheless **must include written State approval for any change to any element that could adversely impact users of the service (public, State or otherwise) or render a State system that utilizes the service unavailable to the system's user community (public, State or otherwise).**

## 5.3 Security as a Service: Authentication and Access Logging and Reporting

### 5.3.1 Authentication/Access Reporting and Logging

Solution must provide authentication and access reports based on any arbitrary attributes the State requires as provided by the underlying software or solution elements.

Solution must support report generation and logging to a State data store for administration tasks, including, but not limited to password resets, granting of privileges, account suspensions, and any other auditing event.

Solution must support report generation and alerting of State Security personnel both directly and via the State's SIEM for security incidents such as, but not limited to, hacking attempts and attempts to access secure resources above an individual's access levels.

The solution must support configuration of Standardized and Ad-hoc reports without requiring any customized programming using common reporting tools such as IBM/Cognos or Tableau which are the State's standard reporting tools.

### 5.3.2 System Operational Reporting, Alerts and Notifications

Solution must include real time mechanisms for monitoring responsiveness, resource consumption, storage utilization, and overall system health.

Solution must include support for intrusion detection and other hacking attempts on identity stores.

Solution must provide real-time notification to administrators and State monitoring staff for performance issues and any security event. Notification must be configurable for email, mobile phone, text messaging, etc.

Alerts need to be configurable by administration staff, not requiring code changes.

The Contractor is responsible for the following Deliverable for this section:

**Deliverable 028.** Master Monitoring and Detection Event Model

- Catalog of All Suspicious and Fraudulent Behaviors and Intrusions
- Tracking and Alerting Framework
- Logging of Systems Access
- Archive / Purge of Systems Access Logs
- Privacy Considerations in Event Logging

## 6.0 State Project Delivery, Management, Methodology and Approach Requirements

The Contractor will provide the State its recommended methodology and approach to the Proof of Concept project and at the request of the State, any Statewide projects that may arise following the successful completion of the Proof of Concept for the State as a result of this RFP.

The Contractor will provide training to State team members on use of the methodology so that State team members may complete their work in accordance with the responsibilities in this RFP.

The State maintains a project management and reporting methodology that is used at varying levels for complex, transformational Information Technology projects. This methodology is designed to provide a substantive and objective framework for the reporting and review of projects to impacted stakeholders and, should the need arise; identify the need for corrective action for one or many of the participants in a project (e.g., State, Contractor, Customer, Stakeholder).

The State acknowledges that various contractors that may do business with the State may maintain unique or proprietary project management methodologies, but seeks to ensure that the overall project is delivered to the State as contracted. Therefore, a minimum standard project management reporting standard has been created to serve the State's project management and oversight needs while not adversely impacting or influencing Contractor provided delivery methodologies.

The Contractor must provide a summary Project Plan as requested by the State. For purposes of a summary project plan specific phase and gate dates, effort and costs are a sufficient minimum.

**Offerors must, at a minimum, include the following deliverables and milestones within their Proposed project plans** and methodologies both within their proposal and at a commencement of the project as a Contractor performing the work following the award of this Contract during the project mobilization phase:

### State Project Management Methodology, Minimum Standards

Phase	Milestone, Activity, Deliverable, Gate	Phase	Milestone, Activity, Deliverable, Gate	
Prioritization and Scheduling	<b>Complete Gate 1 (G1)</b>	Component Test	--> Continued from prior column	
	Create Project Plan		Establish Component Test Expected Results	
	Identify / Secure Resources		Establish Test Plan & Procedures	
	Create Detailed Cost/Time Analysis		Create Test Procedures	
	Create Phasing Strategy / Deliverables by Phase		Execute Component Test	
	Conduct Policy Review		Collect Performance Metrics	
	Initiate Procurement Activities/Plan		Produce Test Analysis Report	
	<b>Complete Gate 2 (G2)</b>		Create Component Technical Documentation	
	Create/Maintain Refined Project Plan		System Integration Test	Establish System Test Expected Results
	Establish Implementation Strategy			Establish UAT Expected Results
Assess Internal/External Project Dependencies	Establish Test Plan & Procedures			
Assess Internal/External Risks	Collect Performance Metrics			
Create Stakeholder/Customer Communications Plan	Produce System Test Report			
Create Detailed Resource Plan	Create System Operational Documentation			
Establish Level 0 System Design	Publish Final Procedures			
Establish/Manage End-User Goals	Create System Technical Documentation			
Determine Existing Process Change Model	Publish Version / Release Document			
Identify New/Enhanced Business Processes	Develop Training Scripts			
Finalize Implementation Strategy	Develop Training Guide			
Analyze Impact to Enterprise Architecture/Data Model	<b>Complete Gate 5 (G5)</b>			
Develop Deployment Strategy	Perform User Acceptance Test			
Finalize Development Tools and Production Requirements	Document/Publish Issue/Bug List			
Validate Customer Adoption Assumptions	Prioritize Issues/Bugs			
<b>Complete Gate 3 (G3)</b>	Create Remediation Effort/Schedule of Outstanding Issues/Bugs			
Follow/Track Final Project Plan	Perform Final Performance and Sizing Testing			
Compile Final Impact Analysis	Create Operational Documents			
Compile Final Risk Assessment	Create User Job Aids			
Create Detailed Design Documents - Functional	<b>Complete Gate 6 (G6)</b>			
Create Detailed Design Documents - Technical	Compile Release Checklist			
Establish Performance Requirements	Update Business Contingency / Continuity Plan			
Establish Operational and Support Requirements	Transition Operational Procedures			
Obtain System Application Software, Tools	Publish Job/Control Schedule			
Create Process Flows with Key Inputs/Outputs	Establish SLA Parameters			
Create Interface Control Documents				

	Create Conversion/Migration Plan	D	Assemble Audit Impact Statement (integrity, security, privacy)	A
	Create Integration Plan	D	Create Release Verification Checklist	D
	Develop Stakeholder Communications Materials	A	Execute Operations Training	A
	Create Solution System Architecture Documents	D	Perform Release Verification	M
	Update Enterprise Architecture Documents	A	Update Enterprise Architecture and Data Model	A
	Create System(s) Sizing Requirements	A	Update Data Center Environments	M
	Establish Test Environment Plan	A	Perform User Training	M
	Establish SDLC Environments	M	Disseminate Documentation and Procedures	A
	<b>Complete Gate 4 (G4)</b>	<b>G</b>	<b>Complete Gate 7 (G7)</b>	<b>G</b>
Component Construction	Develop/Compile Overall Test Plan	A		
	Establish Final Processes	D		
	Develop Test Analysis Report	A		
	Establish Q/A Metrics	A		
	Create/Refine Development Plan	A		
	Develop Code/Solution	D		
	Gather and Report Q/A Metrics	A		
	Develop UAT Plan, Scripts and Cases	D		
	Establish Operational Performance Baseline	M		
	Publish Committed Capacity Plan	A		
	Prepare Component Test Analysis Report	D		
	Develop Training Scripts	A		
Develop Training Guide	A			
	continue to next column -->			

## 6.1 Project Management and Coordination Services

The POC Project will follow the Governance structure defined by the State. Project Management will include the activities to manage the Project including directing the Project Team according to the Project work plan, reporting status, managing issues, assessing quality, leading project meetings, and monitoring schedule and scope changes. The Project Team will produce project status reports on a weekly basis. The format of the status report will be mutually agreed to by the State and the Contractor during the first week of the Project.

The Contractor will:

- Be responsible for the coordination and delivery of the overall Project;
- Ensure that an appropriate “Project Kickoff” occurs and that all integrated work plans are agreed to by the State from project commencement;
- 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;
- 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.

For purposes of the Project, “Perform” means that the party assigned the task has the duty and ultimate responsibility to take all appropriate steps to complete or facilitate the identified task unless otherwise provided for between the parties, subject to the Supporting party completing its interdependent responsibilities. The term, “Support” means that the party has the duty and responsibility to provide ancillary support or assistance which may be necessary to enable the party providing the “Perform” task to complete that task unless otherwise provided for by the parties. If used, the designation, “-” means that the party has no responsibility for the task, unless otherwise agreed by the parties.

Key Tasks	State	Contractor
Conduct Project kick-off meeting	Support	Perform
Create a Work Breakdown Structure (WBS)	Support	Perform
Create and Maintain a project work plan and any related deliverable sub plans	Support	Perform
Review Deliverables and manage the State’s approvals	Perform	Support
Review Deliverables and manage the Contractor’s approvals	Support	Perform
Prepare and conduct project meetings	Support	Perform
Prepare and conduct stakeholder meetings	Perform	Support

Key Tasks	State	Contractor
Create Project Status Reports adhering to the PMO policies	Support	Perform
Report and manage issues and risks	Support	Perform
Monitor and report schedule and scope changes	Support	Perform
Identify State stakeholders and manage expectations	Perform	Support
Assist with on-boarding for the Contractor resources	Support	Perform
Assist with on-boarding for the State resources	Perform	Support
Confirm State Project staffing	Perform	Support
Confirm Contractor Project staffing	Support	Perform
Confirm Project governance	Perform	Support
Initiate Production Acceptance Criteria (“PAC”) process	Support	Perform
PAC – Provide planned checkpoint review dates	Support	Perform

## 6.2 Create and Maintain Project Plan

The Contractor must produce a detailed Project Plan, in electronic and paper form, to the State for approval within twenty business days after the State issues a purchase order or other written payment obligation under the Contract.

### **Deliverable 029.** Master Project Plan

The Master Project Plan should include the following (at a minimum):

- Project Integration;
- Project Scope;
- Project Time;
- Project Quality;
- Project Staffing;
- Project Communications;
- Project Risks/Issues; and
- Project Procurement.

The Contractor must lead a planning session, which ensures the following:

- A common understanding of the Project plan has been established;
- A common vision of all deliverables has been established;
- A common understanding of the 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 defined and agreed to by the State that includes a common understanding of the business, process, technical and other elements of the overall implementation as required.

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.

**At minimum, the offeror must include a Proposed Project Plan(s) as part of its Proposal, which will include the following:**

- **A summary Work breakdown structure;** Scope statement that includes the objectives and the Deliverables and milestones associated with completion of all of the Work with specific provisions for the Work contained and as required by the Proof of Concept project;
- The offeror must provide a single **detailed Project Plan as a Microsoft Project Gantt chart (in native MS Project file “.mpp” format)**, showing all major tasks on a week-by-week schedule, with Proposed Team Members (by name for Key Personnel and by Role for other Project team members) and indications of State participation requirements in the Project(s) to serve as the basis for managing and delivering the Work. The schedule must clearly demonstrate how the project will become fully operational by the delivery date. Within this detailed plan, the offeror must give dates for when all Deliverables and milestones will be completed and start and finish dates for tasks. The offeror also must identify and describe all risk factors associated with the forecasted schedule;
- **The offeror will indicate who (State or Contractor) is assigned responsibility** for each Deliverable within the work breakdown structure to the level at which control will be exercised;
- Performance measurement baselines for technical scope, budget adherence, deliverable assembly, production and approvals in the context of the overall schedule;
- Description of the offeror's proposed organization(s) and management structure responsible for fulfilling the Contract's requirements and supporting the Work, in terms of oversight and control;
- A summary Required State staff and their expected roles, participation and level of effort by project area (e.g., functional, technical, business) as well as role within each Project Phase (e.g., Requirements, Design, Construction, Testing, Deployment);
- Description of the review processes for each milestone and Deliverable (e.g. mandatory design review) and a description of how the parties will conduct communication and status review;
- Description of the Project issue resolution process including an escalation plan; and
- Description of the approach to manage subcontractors effectively, if the Offeror is proposing subcontractors.

### 6.3 Project Review Check Point.

Upon completion of the baselined Project Plan and on a quarterly basis throughout the Contract, the Contractor, in conjunction with State Project team staff, must deliver a presentation to the State. At a minimum, the presentation must address any known State or Contractor issues or concerns, including but not limited to the following:

- Project scope, budget and schedule;
- Any changes to Key named resources assigned to the Project;
- Project readiness including key issues and risk from their current status;
- Project Status including variance from baseline for key milestones, tasks, deliverables (Significant work products) and project closure;

- Methodology, approach, and tools to achieve the Project goals (inventory and status of completeness and agreement for documented project management and implementation approaches. I.e., Project management plan, communication plan, requirements traceability, implementation approach and methodology); and
- Roles, responsibilities, and team expectations.

Upon completion of the presentation, the State will immediately assess the health of the project and determine next steps for moving forward with the Project, within one week of the meeting, which may include the following:

- Continue the Project;
- Terminate the Contract; or
- Suspend the Contract.

See Suspension and Termination language in Attachment Four for remedies for failure to deliver the proposed work.

**Note:** There may be additional Project Reviews conducted by the State on an as needed basis throughout the term of the Contract to assess Project health and ensure the Project is progressing successfully.

#### 6.4 Meeting Attendance and Reporting Requirements.

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

- Immediate Reporting - The Project Manager or a designee must immediately report any Project staffing changes to the State Project Representative;
- Attend Weekly Status Meetings - The State and Contractor Project Managers and other Project team members must attend weekly status meetings with the Project Representative and other members of the 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; and
- 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;
  - Updated Critical Path analysis with the aforementioned GANTT chart and an accompanying PERT chart;
  - 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;
  - The results of any tests;
  - A problem tracking report must be attached;
  - Anticipated tasks to be completed in the next week;
  - Task and Deliverable status, with percentage of completion and time ahead or behind schedule for tasks and milestones;
  - Proposed changes to the Project work breakdown structure and Project schedule, if any;
  - Planned absence of Contractor staff and the expected return date;
  - System integration/interface activities; and
  - The Contractor's proposed format and level of detail for the status report is subject to the State's approval.

#### 6.5 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;
- Store all documents in machine readable, editable and native formats (e.g., XLSx, PPTx, VSD, DOCx) as opposed to proprietary, non-editable, image format or PDF based renderings;
- 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).

## 6.6 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 PaaS environment instance (if applicable). Production deployment includes software deployment to the production instance of the PaaS environment 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 as a deliverable describing Contractor's plan to manage each such implementation.

### **Deliverable 030.** Deployment Plan

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 opinion of the State, 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 as well as perform any data cleansing of legacy data, with the State's assistance, prior to loading data to the new solution;
- 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.

## 6.7 Maintaining Solution and Operations Documentation

For all portions of the solution, as delivered to the State by the Contractor, and thereafter as a result of the Contractor's continued involvement with the Project, the 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 3rd 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; and
- Maintain all documentation on the State's SharePoint site.

## 6.8 Project Delivery, Role and Responsibility Requirements

The State has organized our requirements for responsibilities of the State and Contractor based on the anticipated Activity Areas required to analyze, design, implement and deploy the solution as well as those requirements and activities required to support the deployment of the overall solution. Should an Offeror, as a result of the review of these requirements in light of their proposed approach require additional roles or clarity, the Offeror must indicate the additional requirements of the State and provide a high level rationale for the same as part of their response.

The responsibility matrices included throughout the remainder of this section identify Key Tasks to be performed as part of this project. Each Key Task has been assigned to a party and the level of responsibility for each party is designated as one of "Perform", "Support" or designated "-" for no responsibility.

Note: If the contractor's recommended methodology does not align with the responsibility matrices below, the contractor shall present matrices which do align with the contractor's methodology. The contractor must also demonstrate that the recommended methodology and the responsibility matrices comply with the State's need to: (1) know the contractor has a complete understanding of the State's requirements, (2) the contractor's design and development efforts are in line with the State's requirement for the solution, (3) monitor the contractor's progress during the project, (4) the project risk is acceptable and is managed effectively by the contractor, (5) have accurate and complete technical documentation regarding the solution (as designed and as delivered), and (6)

know the solution delivered and deployed by the contractor has been adequately tested and meets the State's requirements.

## 6.9 System/Environment Administration Support of the Project

The Contractor will coordinate with the State, but be responsible for all environments (production, non-production, demo/training/CRP, development and testing) as required to support the overall effort and will:

- Perform technical activities including but not limited to: version control, Administrative, development, 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.
- 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.

## 6.10 Establish and Manage a Program Management & Master Release Calendar

The Contractor will coordinate with the State in the development, and maintenance on a monthly basis 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.

## 6.11 Cooperation with State and State Contractors

Contractor will cooperate with the State in its attempts at transferring, replacing or augmenting the services responsibilities to another provider in a manner in keeping with not adversely affecting the provision of ongoing services and other projects being performed concurrent with this project.

## 6.12 Requirements Confirmation and Analysis (for each Proof of Concept)

The expectation for this project phase is the Contractor will thoroughly document the desired Security Management business requirements, and elaborate on and confirm all State business, operational, functional and technical requirements and recommend changes which will improve the State's business processes and requirements.

**Deliverable 031.** Confirmed and Agreed to Requirements

## 6.13 Analyze Phase Requirements

The Contractor Team will review, analyze and update the State's Requirements and system(s) documentation. The Contractor team will conduct workshops to confirm with SMEs the results of their business requirements analysis.

The Contractor Team will also analyze impacts to the integration points with external systems. In addition, the Contractor team will analyze external systems and data and recommend data for migration to the solution as applicable.

The Contractor team will deliver the resulting business requirements (expected to be a modified version of the State's current functional requirements), a Requirements Traceability Matrix (RTM), the accompanying business processes modified as required and a list of customizations if applicable. All changes to the State's original functional requirements and business processes are to be clearly indicated.

Key Tasks	State	Contractor
Review and update Business Requirements.	Support	Perform
Document analysis of integration points with external systems.	Perform	Support
Provide functional impacts within external systems.	Support	Perform
Create Requirements Traceability Matrix.	Support	Perform
Create Customization Tracking Database (if applicable).	Support	Perform
Define Technical Requirements.	Support	Perform
Define the solution architecture.	Support	Perform
Document possible solution options for identified gaps, as applicable	Support	Perform
Document plan for integration points.	Support	Perform
Define technical environment requirements for the project from design through deployment and run. This includes any components or tools required to support development, test, configuration management, etc.	Support	Perform
Updated RTM with functional requirements and technical requirements cross referenced.	Support	Perform

**Deliverable 032.** Analyze Phase Document

**6.14 Design Phase Requirements**

The Analyze Checkpoint must be successfully completed prior to beginning any Design phase. This includes the State's acceptance of all deliverables due to date per the project schedule. A validation of the scope and schedule for the remainder of the Project will also be completed at any Analyze or Project Checkpoint.

The Contractor Team will create and maintain Functional Designs for the solution. Functional Designs contain data, business and security impacts and includes integration points to external systems.

Key Tasks	State	Contractor
Create Functional Designs according to the requirements.	Support	Perform
Update Requirements Traceability Matrix with design and configuration cross references	Support	Perform
Create System Test, UAT, and ORT strategies	Support	Perform
Create and update the Technical Designs for solution, including any interfaces to external systems.	Support	Perform
Create and update the Security Designs for the solution.	Support	Perform
Update environment plans for the Project	Support	Perform
Build technology environments required for Build & Test	Support	Perform
Support technical environments, including patches and fixes	Support	Perform
Create Deployment Plan	Support	Perform

**Deliverable 033.** Design Phase Document

**6.15 Build Phase Requirements**

Any Design Checkpoint must be successfully completed prior to beginning any Build phase. This includes the State's acceptance of all deliverables due to date per the project schedule. A validation of the scope and schedule for the remainder of the Project will also be completed at any Design or Project Checkpoint.

The Contractor Team will build the solution and prepare for testing. The State will provide one (1) knowledgeable SME per functional area in test preparation and as mutually agreed to with the Contractor to support test preparation.

Key Tasks	State	Contractor
Provide test conditions and scripts.	Support	Perform

Key Tasks	State	Contractor
Build and Unit Test configuration and security to support the business processes	Support	Perform
Create System Test, UAT, and ORT conditions, scripts, and scenarios	Support	Perform
Prepare testing schedule and participation for System Test, UAT, and ORT	Support	Perform
Create Master Test Plan	Support	Perform
Build and Unit Test the solution as applicable	Support	Perform
Build and Unit Test customizations as applicable	Support	Perform
Build and Unit Test updates to Execution Environment (i.e. interfaces, print, security services, and network infrastructure)	Support	Perform
Build Test Environment(s)	Support	Perform
Build Training environment	Support	Perform
Build Operations Environment (i.e. production)	Support	Perform
Create Assembly Test and Performance Test conditions, scripts, and scenarios	Support	Perform
Support technical environments, including patches and fixes	Support	Perform
Create Deployment and Stabilization Plan and tools (readiness criteria, critical path, and cutover activity list).	Support	Perform

**Deliverable 034.** Build Phase Document

### 6.16 Test Phase Requirements

The Test Readiness Review Checkpoint must be successfully completed prior to beginning any Test phase. This includes the State’s acceptance of all deliverables due to date per the project schedule. A validation of the scope and schedule for the remainder of the Project will also be completed at any Test Readiness Review Checkpoint.

For avoidance of doubt with respect to testing activities, the Contractor is accountable for all activities associated with System Test while the State will participate in these activities. The State is accountable for UAT Test execution while Contractor will be responsible for test preparation, management and tracking of UAT activities.

The Contractor Team will execute System Test, and support the State in performing Operational Readiness Test (“ORT”). The State will provide SMEs knowledgeable in test execution and as mutually agreed to with the Contractor to support test execution.

System Test focuses on the customizations, configurations, workflow and integrations. Test conditions and test scenarios to be included in the System Test will be mutually agreed upon by the Contractor and the State. These scenarios will be based on an analysis of the requirements, changes, and modifications that are approved for implementation.

UAT verifies the usability of the new processes and ensures that the system meets the needs of the State and the end user. UAT leverages System Test Scripts and is executed by State resources. A key objective of UAT is to facilitate an understanding of the technology and the business change being implemented. The Contractor will support the State during the State’s execution of UAT activities.

Prior to production go-live, the Contractor will support Operational Readiness Testing (ORT) that includes end-to-end testing of processes and technologies and will be executed by State members of the Project team. ORT will be conducted during a specific time period before Go-Live.

The State will conduct a Security Test that includes an application scan, manual testing of the system using client-side code analysis, and loading maliciously formatted inbound interface files.

The Contractor Team will develop and prepare weekly Testing status reports to monitor the progress of each test phase. The status reports will contain sections for condition creation, script creation, script execution, issue identification and resolution, and defect identification and resolution.

Key Tasks	State	Contractor
Develop and maintain test data repositories as agreed appropriate	Support	Perform
Manage and track System /Regression Test, UAT, and ORT	Support	Perform
Execute System / Regression Test and document results	Support	Perform

Key Tasks	State	Contractor
Execute UAT	Perform	Support
Document UAT results	Support	Perform
Execute ORT	Perform	Support
Document ORT results	Support	Perform
Prepare for and execute Security Test	Perform	Support
Prepare for and execute Assembly Test	Support	Perform
Prepare for and execute Performance Test	Support	Perform
Support Functional Team Testing	Support	Perform
Conduct Test Moves to Production	Support	Perform
Create the Production Deployment and Stabilization Plan	Support	Perform
Develop, update and maintain a migration checklist	Support	Perform
Prepare for final Move to Production	Support	Perform

**Deliverable 035.** Completion of System Testing

**Deliverable 036.** Completion of User Acceptance Testing

**Deliverable 037.** Completion of Operational Readiness Testing and Final State Acceptance of Solution

The Contractor team will execute System Test and Performance Test.

Moves to Production Test verifies that the technical architecture works together as planned and tests that all elements were migrated to production appropriately. The objective of the Moves to Production Test is to verify that related components function properly when assembled into an overall Solution and work as required by the State.

Performance Test establishes a baseline of acceptable performance for a sample of network and security transactions. The tests are conducted under a practical proportion of expected transaction and user volumes to mimic real-world usability. The sample is based upon State selected data entered into the solution. The number, frequency, and concurrency of network load will be defined using the most recent Contractor team estimates of State network activity available at the time of test preparation. The estimates will be based on State Enterprise-wide usage (as opposed to usage of only the Initial Release Agencies).

The Contractor will recommend a Test Moves to Production strategy as appropriate for their solution's environment(s). The contractor will demonstrate to the State that the strategy allows for the development and testing of a migration process and checklist, as well as an assessment of timing and any mitigation or resolution of any issues related to timing.

Throughout the Project duration, if a testing or production incident is due to errors, omissions, documentation inconsistencies, or bugs in an "in-scope" environment, supported server, or "in-scope" software element licensed by a Third Party to the State, the Contractor will assist the State by referring such incident to the appropriate Third Party entity for resolution and coordinating with the Third Party contractor, as appropriate, to help minimize the State role in problem management.

The Contractor will, to the extent possible, implement measures to help avoid unnecessary recurrence of incidents, by performing root cause analysis and event correlation for items discovered during testing/validation activities.

## 6.17 Deploy Phase Requirements

A Test Completion Checkpoint must be successfully completed prior to beginning any Deploy phase. This includes the State's acceptance of all deliverables due to date per the project schedule.

The Contractor Team will support the deployment activities and will conduct a deployment readiness assessment to determine the readiness of the State and the solution for go-live. Part of the readiness review will be to

determine that the State has reviewed and accepted all functional, technical, and user documentation. Upon the State and Contractor's completion of the readiness assessment, the State will make a final go-live decision. The go-live date will be scheduled and resources, roles, and responsibilities will be confirmed.

Key Tasks	State	Contractor
Identify deployment readiness criteria, critical path, and contingency plan	Support	Perform
Assess deployment readiness	Support	Perform
Define stabilization approach and plan	Support	Perform
Perform deployment activities	Support	Perform
Define end user security mapping and assignments for new or altered functionality	Perform	Support
Create production deployment plan	Support	Perform
Create detailed task lists and work plans for deployment	Support	Perform
Create production deployment staffing schedule	Support	Perform
Create production deployment roles and responsibilities	Support	Perform
Perform cutover activities	Support	Perform
Support technical environments, including patches and fixes	Support	Perform
Coordinate PAC items for Deployment	Perform	Support
Deploy the Solution	Support	Perform
System Turnover	Support	Perform

**Deliverable 038.** Solution Acceptance, State Direction to Deploy to Production

The Contractor Team will drive the planning and execution for the Solution deployment activities. Deployment includes coordination of any required, hardware, appliance, network element or software deployment (as applicable) to the State's infrastructure elements, identification of interfaces and any required conversions/migrations, installation and testing of any required middleware products, installation of server software, and any required testing to achieve the proper roll-out of the application software.

The Contractor Team will execute the deployment plan, which will describe the plan to manage the go-live. The tasks and activities to be performed include the following:

- Execute required system conversions or migrations as applicable;
- Perform required data matching activities and error reporting as applicable;
- Document Solution issues and provide to the State for resolution as applicable;
- Compile and maintain solution issue lists;
- Produce an end-to-end final validation of the operational architecture and corresponding operational documentation for the implemented Solution or System functions (as applicable in the context of a release);
- Conduct 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 Project's life and allow for re-use of such within the State for future Project Phases or upgrades; and
- Transition solution support responsibility according to the Deployment & Stabilization Plan.

**Deliverable 039.** Production Acceptance

The production deployment schedule will be agreed upon mutually by the State and the Contractor.

Production migration activities will adhere to the State Production Acceptance Criteria (PAC) and will not be considered for production migration until all such criteria are met or otherwise accepted by the State. Any deviation, partial acceptance or waiver of requirements in the Production Acceptance Criteria must be agreed to in writing by the State in advance of presentation of any deliverables associated with, or determined to be part of these Production Acceptance Criteria.

Throughout the Project, Application and Tools patches and fixes will be reviewed. Patches will be applied until the QA environment is established. After the QA environment is established and prior to Go-Live, any Application or Tools related patches and fixes will be evaluated for implementation based on the criticality of the patch or fix.

## 6.18 Knowledge Transfer and Production Handoff

The Contractor will perform knowledge transfer support to the State in keeping with State Production Acceptance Checklist (PAC) process which will be made available to the Contractor at the commencement of the project to support knowledge transfer to the State. In general, the PAC will include, at a minimum the following work products as a deliverable:

### **Deliverable 040.** Production Acceptance Checklist

The PAC Deliverable will include, at a minimum:

- Final Requirements Traceability Matrix for the Project as Implemented;
- A list of all customizations and objects as implemented;
- Detailed System Test Cases and Demonstration of Successful Completion of Same;
- Detailed Performance Testing Results showing at least one high volume process (e.g., a Fiscal Quarter or Year or Seasonal Processing as mutually agreed);
- Completion of State User Acceptance Testing and an affirmation of same by State;
- Operational Readiness Testing Results and an affirmation of same by State;
- Complete User and System Administration Documentation that represent the system as implemented; and
- Complete operational documentation sufficient for the State or the State's managed service vendor to operate and maintain the system in the State's environments inclusive of Production, DR, Demo/Train and at least one non-Production replica of the system as delivered.

## 6.19 Project Completion Activities, Final Documentation and Post Implementation Support Obligations

Following one hundred eighty (180) days of successful execution (defined as no Priority 1 or 2 issues) by the Contractor to the State production environment, the Contractor shall be relieved of Project requirements contained herein. During the 180-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 180 day period all defects identified by the State and mutually committed to 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 Priority 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;
  - 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 confirming that all of the above has been delivered and accepted as final.

If, during the 180 day period immediately following the introduction to Production, a Priority 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 180 day period will, at the sole discretion of the State, be reset for additional 180 day periods until such time as the system can perform without Priority 1 and 2 issues.

**Deliverable 041.** Project Completion Certification

## 6.20 Future Project Services Pricing Response and Rate Card

Offerors must provide a Rate Card, by project personnel role and experience level as well as Technical role and experience level that is binding over the Contract term for any Contract change. The Contractor may not propose rates (blended or otherwise) in any Project SOW that differ from this rate card established under any contract arising from this RFP.

## 7.0 Schedule of Deliverables and Work Products

To support the execution of the Project and provide supporting follow-on documentation, the Contractor will create and deliver to the State the following set of Deliverables and Work Products. The State Project Lead will serve as the representative for coordinating respective internal reviews of the subject Deliverable(s) and Work Products for sign off by the State. T

### 7.1 Delivery and Deliverable Standards

- The Contractor will define, document and submit all deliverables they intend to utilize in the performance of this project. Once the State approves these standards, variances to standards must be approved by the State prior to implementation of other than standard practices.
- The Contractor's work and deliverables will be in accordance with the Contractor's State-approved standards (e.g., development methodology, project management, etc.).

### 7.2 Schedule of Key Project Management Work Products

In addition to the deliverables identified throughout this Supplement, the Offeror, as part of their response (as samples) and as Contractor performing the work will provide the following Project Management work products which must be made available to the State for review upon request.

Name	Key Project Management Deliverable / Work Product Descriptions
<b>Kickoff Meeting Presentation</b>	Documents the governance for the Project, roles, approach, timeline, and deliverables in a presentation format to be presented to the Project team.
<b>Project Execution Methodology</b>	This is a detailed description of their project management approach as well as the requirements gathering and analysis, design, build, test, deploy and run methodologies the contractor follows, standards the contractor intends to apply to this project, and any applicable tool sets. Contractor must address topics such as: <ul style="list-style-type: none"> <li>• Financial Controls</li> <li>• Risk and Issue Management</li> <li>• Resource Management</li> <li>• Change Control</li> <li>• Configuration Management</li> <li>• Development Methodology</li> <li>• Test Methodology</li> </ul>
<b>Work Breakdown Structure (WBS)</b>	This document is a hierarchical decomposition of the project into phases, deliverables and work packages. In the work breakdown structure supplied, sufficient detail needs to be presented and maintained over the course of the project to track the earned value against the proposed costs and work efforts. This WBS will be reflected in the Project Workplan.
<b>Resource Plan</b>	The resource plan must specify resources required, by type, over the duration of the project. Contractor must identify all required resources (Contractor, State or otherwise) to complete the project, except where otherwise specified in this document, and include all costs for those resources that are to be provided by the Contractor. Sample roles should be

Name	Key Project Management Deliverable / Work Product Descriptions
	inclusive of Developers, Business Analyst, Administrator, Security Analyst, Database Administrator, or any other roles deemed necessary by the Contractor. The contractor will specify the percent of time each resource will perform their role on State premises.
<b>Organization Structure</b>	<p>This is an org structure reflecting a high-level org structure that incorporates both Contractor and State resources. Roles to address may include any of the following:</p> <ul style="list-style-type: none"> <li>• Sponsors and Stakeholders</li> <li>• Project Management</li> <li>• Quality Assurance</li> <li>• Team Structure and Leads</li> </ul>
<b>Project Workplan</b>	Documents the tasks required to complete the Project, the responsible party for the task, task dependencies, and the resources, duration and work hours required. This plan should include key milestones and phases. The project work plan should be in an acceptable format for the State (e.g., MS Project). The contractor's project manager will work with the State's project manager to ensure an acceptable Project Workplan is completed and accepted as baseline within 20 business days after the Kickoff Meeting.
<b>Change Control Approach</b>	This document must explain the approach for performing change control. This must also include the required communications and coordination points for properly obtaining sign-offs and authorizations.
<b>Overall Solution Requirements and Process Analysis</b>	<p>Documents the results of the requirement and business process analysis and workshop sessions in spreadsheet format, specifically:</p> <ul style="list-style-type: none"> <li>• All recommended changes to the State's original functional requirements and State processes and rationale for the changes.</li> <li>• For each business process gap analyzed, list the functional requirement, standard functionality of the appropriate component of the solution, options to meet the requirement and recommendation</li> </ul>
<b>Gap Analysis</b>	Report documenting gaps between propose solution and requirements, as well as potential solution options to resolve the gaps.
<b>Business Processes &amp; Requirements</b>	<p>The State's security management business processes modified as applicable.</p> <p>The State's functional requirements modified as applicable. In addition, include analysis identifying data migration needs from external systems during deployment</p>
<b>Requirements Traceability Matrix</b>	Lists the requirements for the processes which will be designed and/or built and subsequently tested and deployed. This deliverable will be revised and updated and will be due at each phase check point or as defined in the agreed upon project work plan.
<b>Integration Points Analysis</b>	Defined integration points with external systems to include data analysis, potential for data migration required for deployment and any impacts within the external system.
<b>Customization Tracking Database</b>	This database will track customizations to any commercially developed component of the solution. It will include assessment of the impact to the lifecycle ownership of the component as a result of the customization (e.g., voided warranties, impacts with respect to future commercially available upgrades, patches, etc.).
<b>Solution Architecture</b>	This document defines the application architecture that is to be used during the project and contains the solution architecture (logical and physical). This architecture must show all components and how various systems interrelate, including the external technical environment the solution will operate within.
<b>Capacity Plan</b>	This plan includes the results of the process of determining the operational capacity the solution needs to achieve in order to satisfy the business process demands of the system. It should include planning through the accomplishment of the State's long-term goal of the solution supporting all Security Management within the State, including sub recipient management, sub recipient needs, etc. This document(s) specifies by phase and system the sizing, CPU, and memory requirements.
<b>Technical Requirements</b>	All recommended changes to the State's original technical requirements and rationale for the changes. These requirements should be elaborated upon as required to support the development of the technical specification and design.
<b>Technical Environments Requirements</b>	The identification of all technical environments and the associated requirements, inclusive of all technical environments to be used for the project from the Build Phase through Test, Deploy and Run.
<b>Comm-unication Plan</b>	This specifies typical project stakeholders, communication frequency, and communications vehicles. It must also include the approval process for communications, and how the approval process may differ based on target audience.

Name	Key Project Management Deliverable / Work Product Descriptions
<b>Training Needs Analysis</b>	Identifies the training needs that the target audiences affected by the Project require. Primarily highlights the following: <ul style="list-style-type: none"> <li>• Areas that are changing</li> <li>• Who is affected by the change</li> <li>• Desired level of knowledge and skills expected after the training</li> <li>• Importance or priority of each of the identified processes to the business</li> </ul>
<b>Readiness Plan</b>	Agency/Stakeholder Readiness Plan: Outlines the approach that will be taken to track end user adoption and readiness for the proposed solution, including business process change.
<b>Knowledge Transfer Plan</b>	A plan defining the activities and roles required to perform knowledge transfer of the operations and support of the solution.
<b>Functional Design</b>	Functional design of the solution. Includes the Systems Requirements Document: systems specifications and functional requirements including reliability, performance, operations, usability, maintainability and functional specifications for any interfaces to external systems.
<b>Security Design</b>	Documents the details of the approach that will be followed to meet the identified security requirements of the State.
<b>Technical Design</b>	Documents the technical specifications for the solution to include: <ul style="list-style-type: none"> <li>• Data definitions, identifying any new data elements and classifying new data to be added to the list of confidential and sensitive data.</li> <li>• Unit Test scripts – including both normal and exception processing</li> <li>• Changes to technical architecture</li> <li>• Interfaces to external systems</li> <li>• Any customizations if applicable.</li> <li>• Data Migration from external systems at deployment, if applicable.</li> </ul>
<b>Test Strategy</b>	This is the overall test strategy which includes: <ul style="list-style-type: none"> <li>• Tests to be completed</li> <li>• Test environments</li> <li>• Test tools</li> <li>• Defect tracking</li> <li>• Test approach</li> </ul>
<b>Deployment Plan</b>	Documents the solution deployment approach.
<b>Technology Environments – Build Test</b>	Establish the Technology Environments for Build and Test.
<b>Master Test Plan</b>	This document the plan, scripts (including expected results) and schedule required to execute the various tests phases, including but not limited to System Test, User Acceptance Test, and Performance Test.
<b>Technology Environments</b>	Establish all remaining Technology Environments as defined in the Technical Environments Requirements.
<b>Build and Unit Test Results</b>	Provide build documentation (i.e., changes to code) as a result of unit tests conducted during the Build phase.
<b>Deployment Plan</b>	The plan for deployment of the solution, including tools, readiness criteria and cutover activity list (as applicable).
<b>Training Materials</b>	This includes all training materials and all mediums.
<b>Training Deployment Plan</b>	Documents the plan for rolling out the training to end-users. The Training Deployment Plan lists all the tactical activities that need to occur as training gets rolled out to end-users.
<b>Checkpoint – Test Readiness Review</b>	Documents any difference in the Project scope, schedule, and/or resources at or before the end of the Design Phase. This checkpoint report will focus on the readiness for entering the test phase. Also indicates any deliverables which have not been accepted by the State per the Workplan.

Name	Key Project Management Deliverable / Work Product Descriptions
<b>Deployment Approach</b>	Detailed approach and plan for cutover activities for transitioning the in-scope processes into production. Includes: <ul style="list-style-type: none"> <li>• Deployment preparation</li> <li>• Cutover planning</li> <li>• Stabilization planning for Post Go-Live support.</li> </ul>
<b>Deployment &amp; Stabilization Plan</b>	The plan will cover the timeframe forty-five (45) calendar days before Go-Live and thirty (30) calendar days after Go-Live. This document must identify the series of tasks to be performed in the appropriate sequence to ensure production readiness. This plan must also explain the approach for business continuity during and after cutover. The plans will detail the following for each task: <ul style="list-style-type: none"> <li>• Task name</li> <li>• Owner</li> <li>• Target date for completion</li> <li>• Critical path indicator</li> <li>• The type of tasks will include: <ul style="list-style-type: none"> <li>• Knowledge transfer/training tasks</li> <li>• Operational cutover tasks (i.e., converting data, etc.)</li> <li>• Publish revised policies and procedures</li> <li>• Technical Architecture tasks including readiness, mock deployments and production cutover</li> <li>• Post Go-Live support tasks</li> <li>• Approach for the project team to hand-over long term support to the run support team</li> </ul> </li> </ul>
<b>Data Migration</b>	Test the migration of data from external systems and use the data during testing as applicable.
<b>System Test Results</b>	These documents are the presentation of the results from a particular testing Phase inclusive of substantiation of Contractor testing of all elements as required by the State and contained in the requirements traceability matrix.
<b>Performance Test Results</b>	Documents the results of Performance Test and establishes new performance baselines.
<b>User Acceptance Test Results</b>	These documents are the presentation of the results based on the State's completion of acceptance testing of the Contractor developed upgrade elements. The Contractor will facilitate this deliverable and include identification, classification (i.e., Priority 1-3), and the prioritization of fixing all defects based on State UAT efforts.
<b>Operational Readiness Test Results</b>	Documents the results of the Operational Readiness Test.
<b>Trainer Training</b>	Delivery of training to State's Trainers or Technical Staff as appropriate.
<b>Training Delivery</b>	Completion of the delivery of training per the Training Deployment Plan.
<b>System Deployed</b>	This is the acceptance of the State deployment checklist for Production and Non-Production environments.
<b>System Turnover</b>	Transition solution support responsibility per the Deployment & Stabilization Plan. This includes Knowledge Transfer Activities per the Knowledge Transfer Plan.

## 8.0 Assumptions

The offeror must list all the assumptions 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.**

### 8.1 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.

## 8.2 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.

## 8.3 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.

## 9.0 State Staffing Requirements

As this project is an Enterprise offering supported by DAS/OIT and includes Agency participation in the Proof of Concept Project identified herein, the following table represents the State's minimum commitments to this Project. Should, based on the experience of the offeror additional roles be required of the State, the offeror will identify these roles, provide rationale and include a summary description of the skills and competencies required for each position. Note all roles (State minimum or otherwise) must be included in the offeror Staffing Plan as required in this section of the Supplement. For all State roles marked "as required" offerors are to include (within their proposal) the staffing level required of the State to ensure that the Contractor project is supported adequately.

The State will provide a dedicated State Project Lead to serve as the Contractor's day-to-day point of contact for the Project. This role will be staffed throughout the duration of the Project. The State Project Lead will facilitate process and policy decisions in support of the Project schedule. State personnel assigned to the Analyze Phase

will maintain consistent involvement throughout the duration of the Project. These individuals will be accessible and available to participate as agreed upon in the approved Project Plan.

Project Area	State Trust Ohio Core Team (DAS/OIT)
Overall Project Management	1 FTE
State Standards Lead: State Policy and IT Standards	1 PTE as required (advisory)
Security Advisor (State CISO Office)	1 FTE (design phases), part-time advisory thereafter
Privacy Advisor (State CIPO Office)	1 FTE (design phases), part-time advisory thereafter
Security/Privacy SME	Up to 1 FTE as required
State Network Lead	Up to 1 FTE as required
State Cloud Technical Lead	Up to 1 FTE as required
State SIEM Integration and Reporting	Up to 1 FTE as required
System Test Lead	As required
System Test Participants	As required
State Infrastructure Liaisons	Up to 4 PTE (Network, Server, Storage, Directory) as required

### 9.1 Contract Staffing and Key Activities

The offeror is to consider the roles provided by the State as well as those proposed that are required for the Proof of Concept Project 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 phase), 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., Project Manager, business analysis, technical lead, functional lead, etc.). Offerors are to propose a combined team organization (i.e., State and Contractor) designed to deliver the project to the State as per the requirements in this Supplement.

#### Offeror Team Organization, Key Personnel and Work Location(s) –Proof of Concept

Role #	Contractor Role	Role Activity	FT/PT	% Time On Site
<b>Analyze Phase</b>				
		[insert rows as required]		
<b>Design Phase</b>				
		[insert rows as required]		
<b>Build Phase</b>				
		[insert rows as required]		
<b>Test Phase</b>				
		[insert rows as required]		
<b>Deploy Phase</b>				
		[insert rows as required]		
<b>Post Implementation Support</b>				
		[insert rows as required]		

## 9.2 Staffing Plan and Time Commitment

The offerors Staffing Plan and Time Commitment response must contain the following information:

- An organizational chart including any subcontractors and key management and administrative personnel assigned to this project.
- A contingency plan that shows the ability to add more staff if needed to ensure meeting the Project's due date(s).
- The number of people onsite at State location(s) at any given time to allow the State to plan for the appropriate workspace. **Offeror Note:** The following table is provided as an **example** of what the State expects the offeror to provide in the proposal response for this requirement.

**Illustrative Offeror Staffing Plan**

Project Month	1	2	3	4	5	6	7	8	9	10	11
Phase	Startup / Analyze	Design Phase			Build Phase		Test Phase		Deployment		Operate
Project Management											
State	3	3	3	3	3	3	3	3	3	3	3
Contractor	2	2	2	2	2	2	2	2	2	2	2
Functional FTEs											
State	4	4	4	4	4	4	4	4	4	4	4
Contractor	8	8	8	8	8	8	8	8	8	8	8
Technical FTEs											
State Infrastructure	2	2	2	2	2	2	2	2	2	2	2
State Security	1	1	1	1	1	1	1	1	1	1	1
Contractor	6	6	6	6	6	6	6	6	6	6	6
Business / Agency FTEs											
State	4	4	4	4	4	4	4	4	4	4	4
Contractor	2	2	2	2	2	2	2	2	2	2	2
Summary Total											
State	14	14	14	14	14	14	14	14	14	14	14
Contractor	19	19	19	19	19	19	19	19	19	19	19

Offerors are encouraged to add additional roles and responsibilities as appropriate based on their proposed Project Staffing Plan as to highlight the involvement of their Proposed Team and inclusion of State resources in the project to help ensure its success. The number of FTEs depicted in the above table are provided as an **illustrative example** and in no way connotes State expectations as to the level or involvement of the State or Contractor in this project.

A statement and a chart that clearly indicates the time commitment of the proposed Project Manager and the offeror's Key Project Personnel, inclusive of the Project Manager and the offeror's proposed team members for this Work during each phase of the Projects, the System Development Life Cycle associated with Projects, and the commencement and ongoing operation of the within the Service.

- The offeror also must include a statement indicating to what extent, if any, the candidates may work on other projects or assignments that are **not** State related during the term of the Contract. The State may reject any Proposal that commits the proposed Project Manager or any proposed Key Project 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 Project Personnel who will provide services as part of the resulting Contract. The Key Project Personnel are identified in each applicable Supplement. The State expects that the proposed named Key Project Personnel will be available as proposed to work on the Project. Resumes for the proposed candidates must be provided for all Key Project 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

### 10.0 Service Level Requirements: Security as a Service

The following Service Levels shall apply to the ongoing operation of the overall Service.

#### 10.1 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		(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		(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		\$6,960.00		\$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.

## 10.2 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 Multiplier 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.**

### 10.3 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.**

### 10.4 Service Availability

Service Availability for each in-scope element provided by the Contractor that the State utilizes commercially supporting State system operations, development and maintenance activities, training, demonstration or supporting non-commercial use application usage.

**Standard:** 99.99% available, 24 hours per day, 365 days per year less mutually agreed to scheduled maintenance windows not to exceed one hour per month.

### 10.5 Priority 1 Outage Resolution Time

Priority 1 Outage means that there is a Critical Function outage causing severe impact on service delivery and no alternative or bypass is available. The Service Provider will provide notice of Priority 1 incidents along with a preliminary diagnosis and estimated resolution time within 15 minutes of detecting the Incident or being informed by the State of such outage.

A severe impact means: The Incident renders a business critical function, System, Service, Software, Equipment or network component un-Available, substantially un-Available or seriously impacts normal State operations, in each case prohibiting the execution of productive work.

**Standard:** Detection of Outage and Reporting to State estimated time of resolution: 15 Minutes, resolution of outage and return to contracted standards within 60 minutes.

## 10.6 Service Level Specific Performance Credits

Failure to meet any Service level contained in this Section in a given month shall result in a 5% fee credit of the total monthly charges to the State for the Service month following each failure to meet the contracted standard(s) identified by the State or Contractor.

## 11.0 Service Level Requirements: State Systems Integration 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 (asset or cloud-based) associated with this Supplement in general, and under Section 5.0 specifically as the work pertains to any Enterprise or Agency Projects or subsequent or Additional Work for State Agencies.

The section contains the tables and descriptions that provide the State Service 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.

## 11.1 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	1st Month		2nd Month		3rd 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		(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		(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		\$6,960.00		\$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.

### 11.2 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.**

### 11.3 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.**

### 11.4 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 – Priority 1 Items	SLA	7x24	Every 4 hours until resolution	<= 24 hours
Defect Resolution – Priority 2 Items	SLA	7x16	Every 8 hours until resolution	<=72 hours
Defect Resolution – Priority 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	-

## 11.5 Service Level Specifications

### 11.5.1 Defect Resolution – Mean Time to Repair/Resolve (Priority 1 Items)

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

**Definition:** Mean Time to Repair (Priority 1 Items) will be calculated by determining time (stated in hours and minutes) representing the statistical mean for all Priority 1 Defects for in-scope deliverables in the Contract Month. “Time to Repair” is measured from the time an 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. “Priority 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 (Priority 1 Outages) = 
$$\frac{\text{(Total elapsed time it takes to repair Priority 1 Defect Service Requests)}}{\text{(Total Priority 1 Defect Service Requests)}}$$

**Measurement Period:** Month

**Data Source:** Monthly Project Report

**Frequency of Collection:** Per Incident

#### Service Level Measures

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

## 11.5.2 Defect Resolution – Mean Time to Repair/Resolve (Priority 2 Items)

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

**Definition:** Mean Time to Repair (Priority 2 Items) will be calculated by determining time (stated in hours and minutes) representing the statistical mean for all Priority 2 Defects for in-scope deliverables in the Contract Month. “Time to Repair” is measured from the time an 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.

“Priority 2 Defect Service Request” means an incident caused by the Software or a 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:**

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

**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 (Priority 2 Defects).
Green	<= 72 hours
Yellow	> 72 hours and <= 90 hours
Red	> 90 hours

### 11.5.3 Defect Resolution – Mean Time to Repair/Resolve (Priority 3 Items)

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

**Definition:** Mean Time to Repair (Priority 3 Items) will be calculated by determining time (stated in hours and minutes) representing the statistical mean for all Priority 3 Defects for in-scope deliverables in the Contract Month. “Time to Repair” is measured from the time an 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.

“Priority 3 Defect Service Request” means an incident caused by the Software or a 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 Priority 1 or Priority 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:**

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

**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 (Priority 3 Defects).
Green	<= 7 calendar days
Yellow	> 7 calendar days and <= 10 calendar days
Red	> 10 calendar days

## 11.5.4 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 priority), 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 Priority 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%

## 11.5.5 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:**

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

**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%

## 11.5.6 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:**

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

**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 SL GYR State	Issue Find/Fix Rate
Green	<= 10%
Yellow	>10%, <= 12%
Red	<= 15%

## 11.5.7 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:**

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

**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%

## 11.5.8 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:**

$$\% \text{ Compliance, Milestone Dates} = \frac{\text{Total Number of Contractor Milestones met within the measurement month}}{\text{Total Number of Contractor Milestones planned to be met during the measurement month per the agreed upon list of milestones}} \times 100$$

**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%

## 11.5.9 Issue Reporting

**Specification:** % Compliance Issue Reporting

**Definition:** The reporting of any issues impacting the Project to the State for prompt resolution and possible solutions. 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:**

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

**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%

## 11.5.10 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:**

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

**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%

## 11.5.11 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%

## 11.5.12 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:**

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

**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%

### 11.5.13 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:**

$$\text{\% Estimating Accuracy} = \frac{\text{Time Spent in Build and Testing Activities Actual Number of Work Units Submitted in a Month (cumulative for phase or release)}}{\text{Actual Work Units Total Project Time (Hours) Spent During Build and Test Periods (i.e., Total Time)}} \times 100$$

**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
<b>Green</b>	>75%
<b>Yellow</b>	>70%, <=75%
<b>Red</b>	<= 70%

## 11.5.14 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 90 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 90 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 90 days, whichever is longer.

**Formula:**

$$\frac{\text{Issues Identified and Resolved in Production}}{\frac{\text{Total Time Required to Resolve Issues Identified During initial 90 day production Period}}{\text{Total Hours included in a Production Release}}} \times 100$$

**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%