

SUPPLEMENTAL INFORMATION HEADER

The following pages contain supplemental information for this competitive document. The supplemental information is contained between this header and a trailer page. If you receive the trailer page, all supplemental information has been received.

If you do not receive the trailer page of this supplement, use the inquiry process described in the document to notify the Procurement Representative.

Note: portions of the supplemental information provided may or may not contain page numbers. The total number of pages indicated on the cover page does not include the pages contained in this supplement.

Supplement 1: Requirements and Statement of Work

Enterprise Imaging Framework Solution

DAS HRD Imaging Project

Contents

Supplement 1: Requirements and Statement of Work	1
1.0 Solution Overview and General Scope	5
1.1. HRD Implementation, Conceptual Proof of Framework and Future Project Opportunities	5
1.2. Conceptual Grouping of State Requirements, Framework Context.....	6
1.3. Asset Based Solution	8
2.0 Project Management Requirements (Applies to All Elements of this RFP)	8
2.1. Project Management Scope	8
2.2. Document Convention: Deliverable Identification	9
2.3. State Project Team Organization	9
2.4. Create and Maintain Project Plan	10
2.5. Meeting Attendance and Reporting Requirements	10
2.6. Develop, Submit, and Update Detailed Activity Plans	11
2.7. Utilize OIT's Document Sharing/Collaboration Capability.....	11
2.8. Project Management Methodology, Minimum Standards	12
2.9. System and Acceptance Testing Requirements	14
2.10. Performance and Reliability Testing Requirements	15
2.11. System Changes as a Result of Contractor Activities.....	15
2.12. Project Solution Implementation Considerations and Requirements.....	16
2.13. Project System Environments	16
2.14. Change Management/Communications and User Training	17
2.15. Design Phase Responsibilities and Deliverables.....	18
2.16. Construction Phase Responsibilities and Deliverables.....	18
2.17. Testing and Acceptance Phase Responsibilities and Deliverables	19
2.18. Pre-Production/Production Deployment Phase Responsibilities and Deliverables	19
2.19. Post Implementation Support Responsibilities and Deliverables.....	20
3.0 HRD Document Imaging Requirements.....	22
3.1. Objectives and Overview.....	22
3.2. Context Diagram: HRD Requirements and Overall Enterprise Framework.....	22
3.3. Organizational Overview	23
3.4. Required Implementation Timelines.....	24
3.5. State Personnel Record, Logical Mapping, Hierarchy and Data Elements	24
3.6. Current State HR Operations State Personnel Records Unit	25
3.7. Architecture Overview and Volumetric Information: Current HRD Personnel Records Systems	25
3.8. HRD State Personnel Records Repositories	26
3.9. HRD Users and General Responsibilities	27
3.10. Current State – Agency Human Resource Departments	28
3.11. General HRD System Requirements	29

3.12.	High Volume Offsite Imaging Services Requirements	29
3.13.	Agency HR Department General Requirements	30
3.14.	Agency Migration Requirements	31
3.15.	DMS Integration Diagram	31
3.16.	Required Operating Environment and OAKS Integrations.....	32
3.17.	DMS Usage Scenarios by HRD and Agencies	32
3.18.	Requirements and Sizing: Document Migration from Existing DMS Platforms	33
3.19.	HRD Imaging Requirements Matrix	34
3.20.	HRD Solution Requirements Matrix	35
3.21.	HRD Roll-Out Plan, Suggested Phasing.....	81
3.21.1.	Phase 1 – HRD and Pilot Agency Elements	81
3.21.2.	Phase 2 Outside Agency Elements.....	81
3.21.3.	Phase 3 Future Implementation for Outside Agency Elements	81
3.21.4.	Out of Scope	82
3.22.	Use Cases	82
3.22.1.	On Boarding Process	82
3.22.2.	Employee Transfer	82
3.22.3.	ePAR.....	82
3.22.4.	ePerformance.....	82
4.0	State Infrastructure, Operations Integration and Use Requirements.....	83
4.1.	System Access: User Accounts	83
4.2.	Operational Requirements	83
4.3.	Disaster Recovery & Backups.....	83
4.4.	Policy Compliance	83
5.0	Post Project Production Transition Requirements	84
6.0	Application Maintenance and Applications Operations Requirements	85
6.1.	Post Implementation and Long Term Support	86
6.2.	Steady-State Operations and Maintenance Services (Run Services)	87
6.3.	Assist the State with Help/Service Desk Services Specific to the Solution	87
6.4.	Incident / Problem / Change (I/P/C, ITIL) Management.....	88
6.5.	Additional Services	89
6.6.	Job Execution / Production Control.....	89
6.7.	Break/Fix Support.....	90
6.8.	Environment Technical Support	91
6.9.	System/Environment Administration Support.....	91
6.10.	Systems Management and Administration.....	92
6.11.	System Environment Maintenance	92
6.12.	Environment Management (Production, Development, System Testing/QA, , Demo/Train,).....	93

6.13.	Problem Management Services	94
6.14.	Service Reporting	94
6.15.	Maintaining Solution and Operations Documentation	94
7.0	Service Level Agreements and Contractor Fee Credits	95
7.1.	Service Level Framework	95
7.2.	Service Level Specific Performance Credits	95
7.3.	Treatment of Federal, State, and Local Fines Related to Service Disruption	97
7.4.	Overall Contract Performance	97
7.5.	Monthly Service Level Report	98
7.6.	Period Service Level in Full Effect and In-Progress Service Levels	98
7.7.	Service Levels Review	98
7.8.	State Provided Service Support Infrastructure Elements	99
7.9.	Imaging Managed Service: Service Level Commitments	99
7.9.1.	Incident Resolution – Mean Time to Repair (Priority 1 Outages)	100
7.9.2.	Incident Resolution – Mean Time to Repair (Priority 2 Outages)	101
7.9.3.	Incident Resolution – Mean Time to Repair (Priority 3 Outages)	101
7.9.4.	Service Availability – Application Availability	102
7.9.5.	System Performance and Responsiveness	103
7.9.6.	Incident Resolution - Issue Triage, Closure and Recidivist Rate	104
7.9.7.	Security – Security Compliance	105
7.9.8.	Security – Monitoring & Auditing – Security Breach Detection	106
7.9.9.	Job Schedule and Scheduled Reporting Performance	107
7.9.10.	Service Quality – System Changes	107
7.9.11.	Service Timeliness – System Changes	108

1.0 Solution Overview and General Scope

The State, via more than 120 Agencies, Boards and Commissions has a variety of requirements that need to be fulfilled by imaging/workflow/integration solutions that are specific or related to the business needs of the State and aligned with the missions of each Agency, Board and Commission. Specific to the requirements of the Department of Administrative Services (DAS) Human Resources Division (HRD), there is a need to identify, select and implement an extensible platform that is suited to the requirements of HRD and the state HR Community, but extensible and applicable to other near term imaging and workflow requirements associated with large scale systems integration projects. The State seeks to identify such a solution via this RFP to:

- Address HRD's immediate needs and requirements contained in this RFP;
- Serve as a basis for ongoing standardization for other systems requirements;
- Provides an extensible enterprise platform that is "image source" and "target system" integration agnostic;
- Flexible and extensible to address high volume imaging, transaction processing, storage, retrieval and integration requirements of any Agency;
- Can be implemented in a modular fashion that allows the State to leverage existing investments and deployments in scanning technology and services, workflow, document management, storage, networks and open systems based on modern APIs and integration format capabilities; and
- Requires modest investment from an enterprise perspective that makes financial and business sense with respect to the initial implementation for HRD, and subsequent addition of new opportunities as they are identified by the State.

1.1. HRD Implementation, Conceptual Proof of Framework and Future Project Opportunities

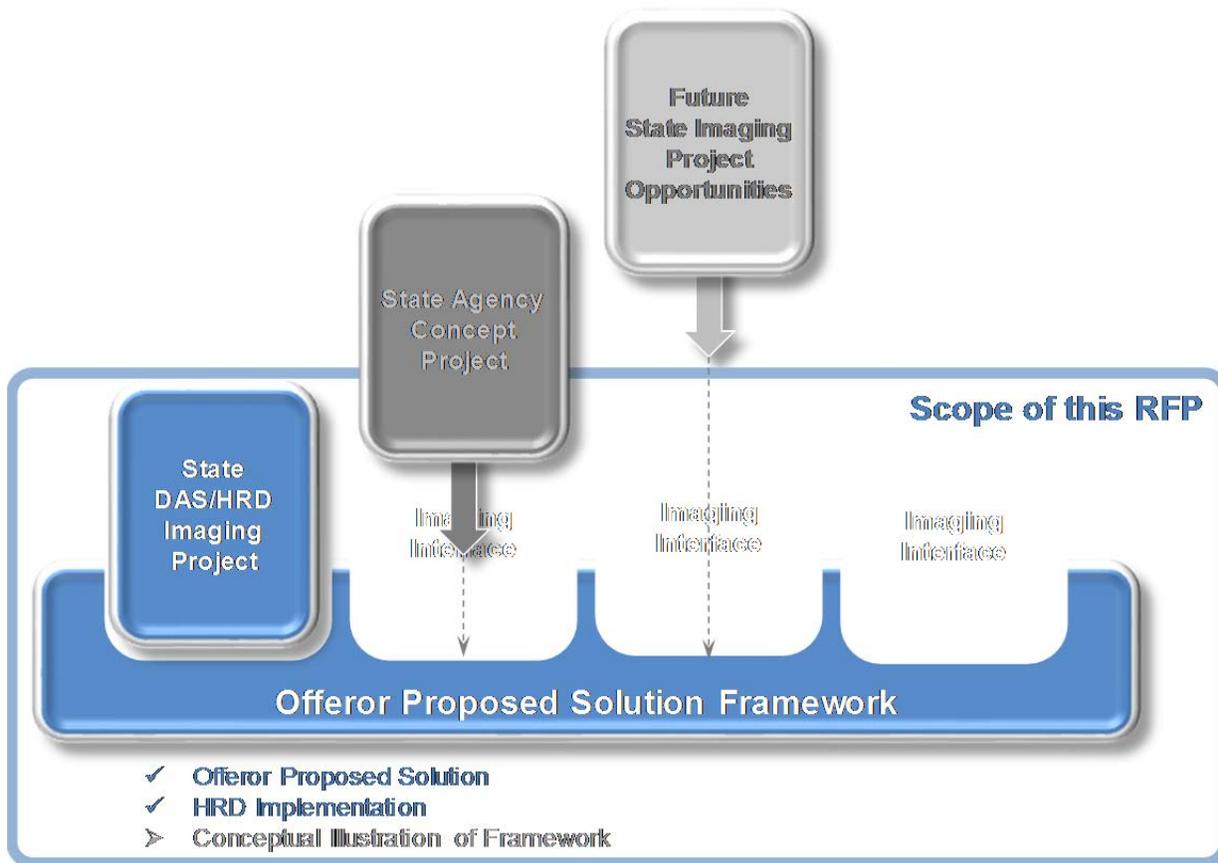
This RFP contains and will be evaluated upon criteria contained in the Base RFP and requirements in this Supplement and Supplements 2 and 3. As a general summary, the State will evaluate using the following considerations:

- **Compliance** with the design, implementation and production use of HRD's requirements contained in this Supplement;
- As HRD data contains personal and sensitive employee data (e.g., benefits, compensation, enrollment and performance forms), compliance with **State Security and Data Handling Requirements** from a proposed solution and implementation perspective are essential (as contained in Supplement 3);
- **Extensibility** of the proposed solution to meet other situational needs of the State as a "proof of framework" using conceptual requirements of a State Agency that may have near-term needs to utilize the proposed platform in a similar fashion to those required by HRD;
- **Modularity** of the proposed solution to allow the State to selectively implement elements of the solution in a variety of systems support roles that leverage existing or future State investments in scanning, imaging, workflow, routing, storage and integration with State systems in the future; and
- **Flexibility and Adaptability** of the solution to:
 - Address a variety of image inputs (forms, formats and standards);
 - Accept presentation from a variety of sources (desktop scanners, workgroup imaging platforms, high volume imaging platforms or managed imaging vendors);
 - Align with specific situational business needs (e.g., HR data, Business data, State revenue data, citizen data) based on the mission of an Agency and it's needs; and
 - Integrate with existing or new State systems using available APIs based upon open-standards such as XML, SOAP, .NET and other integration frameworks.

As a general overview of the State's view of these framework requirements, the following diagram is designed to illustrate the specific scope of the HRD implementation requirements which are contained in this Supplement and will be the basis of any work arising from this RFP and it's award; conceptual requirements for a large State

Agency that are designed to allow the State to evaluate the proposed framework and potentially extend the work under this RFP to include those requirements; and consideration for the inclusion of future Agency work pending need and alignment with the proposed solution to the requirements of a future State Agency project.

Conceptual Overview: Proposed Solution Framework and Scope of this RFP

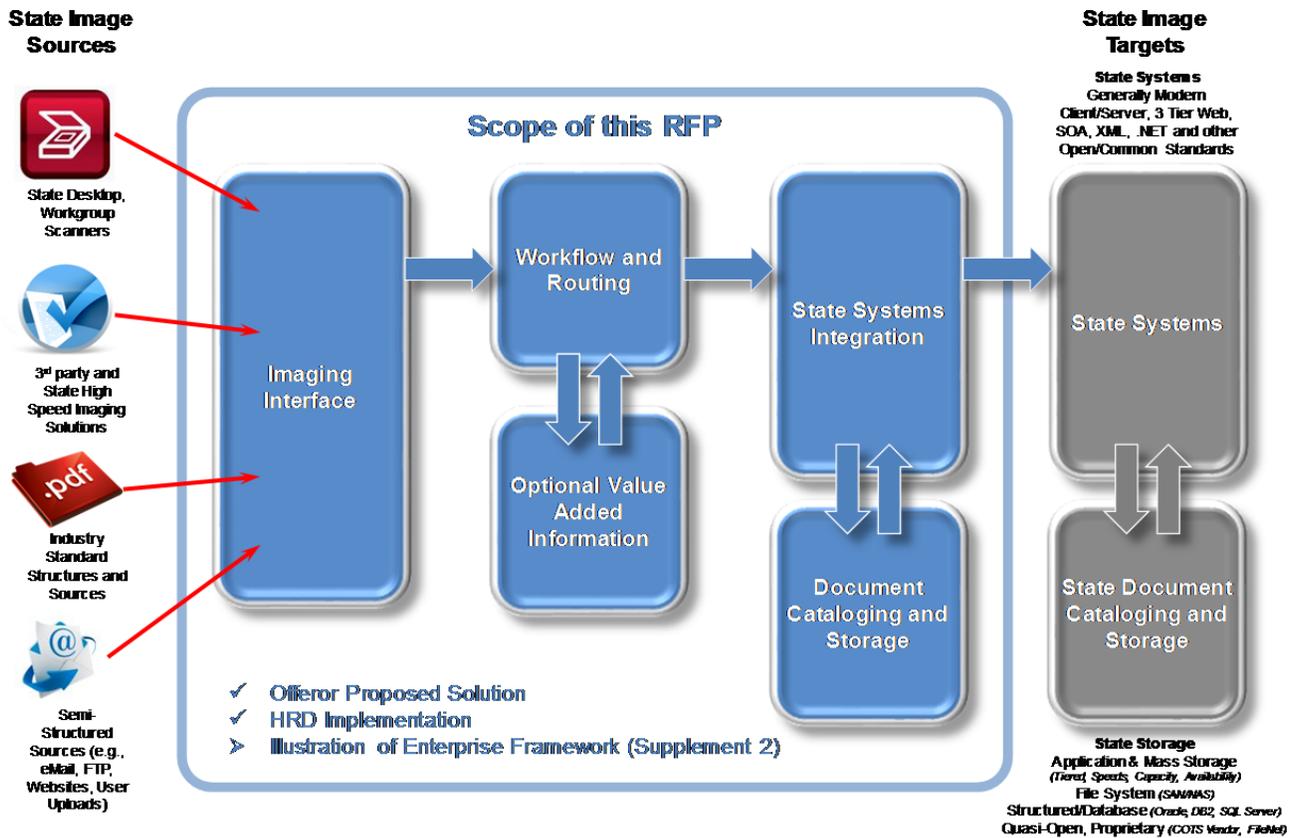


Elements in **BLUE** are the specific implementation scope of this RFP; those in **GRAY** are out of the implementation scope of this RFP. The State requires an Offeror response to all elements contained in this RFP.

1.2. Conceptual Grouping of State Requirements, Framework Context

The State has no preconceived notion as to the architecture, components or organization of the Offeror’s proposed solution as long as the Framework and HRD requirements are met and implemented as contained in this RFP. By way of a conceptual grouping of both the HRD and Framework requirements contained herein, the State offers the following diagram to organize its requirements for convenience of a common basis of communication and articulation of its views as to the context of the overall solution (in general) and specific to the needs of HRD and other identified Agency opportunities.

Conceptual Organization of Solution Requirements: Framework Context and Opportunities



Specific State functional and technical requirements for the HRD and Imaging Framework are contained later in this Supplement; general descriptions of each element of this conceptual organization diagram are as follows:

Framework / Solution Organization Area	Illustrative Attributes and Elements
State Image Sources	<ul style="list-style-type: none"> Agency specific imaging platforms from a variety of Original Equipment Manufacturer (OEM) vendors. Desktop/Workgroup imaging sources such as scanners, multifunction copiers, etc. Citizen/Business/Vendor scanned forms and documents provided to the State via email, electronic gateways and other mechanisms. Industry standard structured formats including PDFs, XML, embedded forms, bar codes, Microsoft Office, TIFF, etc. Semi-Structured Data using a variety of sources, formats and transmission mechanisms that may include structured forms with handwritten augmentation (e.g., a W4 withholding form or signed document).
Imaging Interface	<ul style="list-style-type: none"> Offeror proposed system elements to accept State Image Sources into the Offeror proposed solution. Offeror provided solution elements to provide images to its solution in the absence of a compatible or acceptable State image source (for example, those imaging requirements that cannot be met by an existing image source or where an image source is unavailable at the point of image origination).
Workflow and Routing	<ul style="list-style-type: none"> Elements of the Offeror solution that “guide” the image through the required State processes and work-steps. Initial error identification/rejection/recycling, prioritization and distribution to State workgroups (domain generalists and specialists). Routing to transaction processing groups.

Framework / Solution Organization Area	Illustrative Attributes and Elements
	<ul style="list-style-type: none"> ▪ Integration with State systems as required and agreed with the State.
Optional Value Added Information	<ul style="list-style-type: none"> ▪ Optical character recognition. ▪ Image metadata tagging used to identify origin, use, purpose, destination and processing considerations. ▪ Data classification based on origin/type of data (e.g., PII, financial, banking, HIPPA, IRS, etc.). ▪ Image to Business/Employee/Citizen matching considerations to streamline processing, workflows, cases and integration. ▪ Barcoding, watermarking, dating, versioning and other image enhancements. ▪ Digital signature identification and capture.
State Systems Integration	<ul style="list-style-type: none"> ▪ Integration frameworks that are designed to format the data in structures and formats compatible to integrate from the source State systems to the target imaging system. ▪ Interface/integration controls to ensure that integration(s) occur as required and that no data, images or information is lost in translation or transit. ▪ Maintaining a variety of image formats and integration methods based on industry standards that ensure that images and information are useful as a companion to, or as part of a State system.
Document Cataloging and Storage	<ul style="list-style-type: none"> ▪ For those State systems that do not have the capability or provision for large scale image storage management, accommodation of storage image data stores that maintain this data in a manner that appears seamless to a State end-user in performance of process responsibilities. ▪ Cataloging of all images with controls to adhere to data privacy, access, security and other requirements in consideration of the contents of the images. ▪ Data structures that can be used independent of a State target system to inventory, maintain, archive and purge these images upon reaching their practical or useful life.
State Systems	<ul style="list-style-type: none"> ▪ Detailed integration and data exchange requirements specific to a State solution ▪ Timing, format, technology and other technical elements as required by a State system specific to the imaging requirement set.
State Document Cataloging and Storage	<ul style="list-style-type: none"> ▪ Specifics as to what, how and how much data can or will be maintained in a State system as opposed to the Offeror provided Document Cataloging and Storage capability. ▪ Integration requirements and capabilities between a given State System and the Offeror proposed system

1.3. Asset Based Solution

Asset Based Solution. The State has preference for Asset Based Solutions for this framework. Asset based solutions are those in which Offeror proposed solutions that require the State to acquire, license and maintain computing assets including, but not limited to; servers, storage, network connectivity and other tangible elements that the State must acquire or license and subsequently maintain and operate. Offeror's will include a Bill of Materials (BOM) and total costs as part of their proposal to the State. Upon acceptance of the final solution, the Contractor will transfer all assets to the State, inclusive of support and maintenance contracts and obligations.

Notwithstanding the Offeror proposed solution under the aforementioned classifications, the solution must:

- Demonstrate adherence to all requirements in this RFP and it's Supplements;
- Include **all** costs required to design, implement, operate and maintain the solution based on the requirements herein and provisions of this RFP; and
- Include in a detailed bill of materials in the Cost Workbook all elements that the State must acquire by way of hardware, storage, scanning, networking and other infrastructure to utilize the solution as proposed.

2.0 Project Management Requirements (Applies to All Elements of this RFP)

2.1. Project Management Scope

The Contractor will have responsibility to provide overall project management for the task areas in this Supplement, specifically the implementation of an Imaging Solution that meets the requirements contained in this RFP.

The Contractor will:

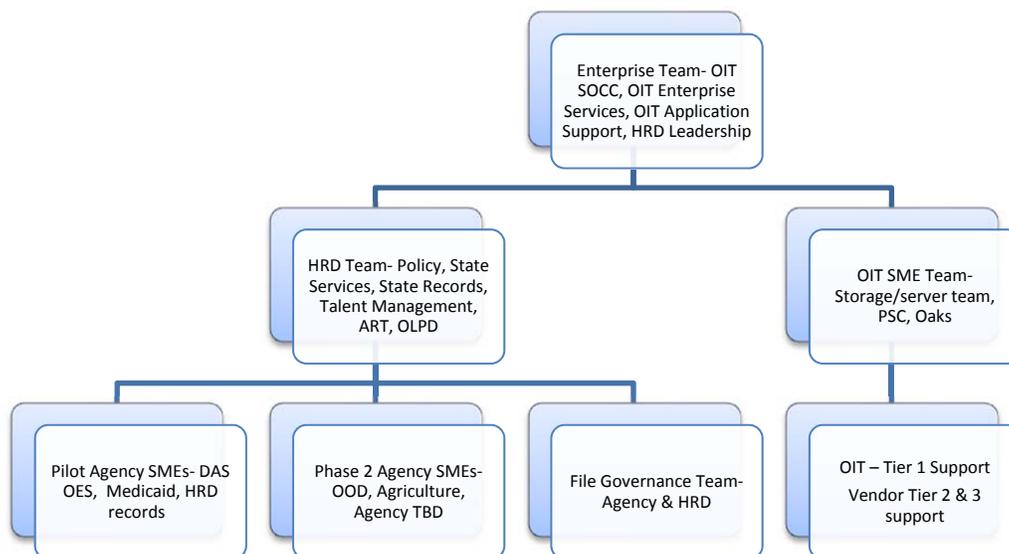
- Be responsible for overall Project completion;
- Maintain the overall Project Plan;
- Ensure deliverables have a detailed project sub plan as required by the State to ensure timely delivery and appropriate quality;
- Ensure that all efforts have an effective version control mechanism for all documents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

2.2. Document Convention: Deliverable Identification

All items in this Supplement that are marked with a red star (★) shall be considered formal deliverables and be subject to the State’s deliverable acceptance process described in Part 2: Special Provisions, Submittal of Deliverables of the RFP.

2.3. State Project Team Organization

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



2.4. Create and Maintain Project Plan

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

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

Thereafter, the Contractor must:

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

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

2.5. Meeting Attendance and Reporting Requirements

The Contractor's project management 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 Manager.
- Attend Weekly Status and other Key Meetings - The State and Contractor Project Managers and other Project team members must attend weekly status meetings with other members of the Project teams on State premises as deemed necessary by the State 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 State Project Manager by close of business on Thursday of each week before each weekly status meeting.
- At a minimum, weekly status reports must contain the items identified below:
 - Updated GANTT chart, along with a copy of the corresponding Project Plan files (i.e. MS Project) on electronic media acceptable to the State;
 - Status of currently planned tasks, specifically identifying tasks not on schedule and a resolution plan to return to the planned schedule;
- Issues encountered, proposed resolutions, and actual resolutions;
 - 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;

- Identification of Contractor staff assigned to specific activities;
 - Planned absence of Contractor staff and the expected return date;
 - Modification of any known staffing changes; and
 - System integration/interface activities.
- The Contractor's proposed format and level of detail for the status report is subject to the State's approval.
 - Prepare Monthly Status Reports – During the Project, the Contractor must submit a written monthly status report to the State Project Manager by the fifth business day following the end of each month. At a minimum, monthly status reports must contain the following:
 - A description of the overall completion status of the Project in terms of the approved Project Plan (schedule and cost, if applicable);
 - Updated Project work breakdown structure and Project schedule;
 - The plans for activities scheduled for the next month;
 - The status of all Deliverables, with percentage of completion;
 - Time ahead or behind schedule for applicable tasks;
 - A risk analysis of actual and perceived problems;
 - Testing status and test results; and
 - Strategic changes to the Project Plan, if any.

2.6. Develop, Submit, and Update Detailed Activity Plans

As part of the Project and no later than twenty business days following the commencement of the effort, the Contractor must develop a Project Management Plan (Project Plan). The Contractor also must update the plans with more detail throughout subsequent Project phases coincident with Project Status reports or upon reasonable request of the State Project Manager to address, at a minimum, the following subjects:

- ★ Project Plan including (at a minimum):
 - Project Integration;
 - Project Scope;
 - Project Time;
 - Project Quality;
 - Project Staffing;
 - Project Communications;
 - Project Risks/Issues; and
 - Project Procurement.

The Offeror must develop these plans from information that the State's Project personnel provide. These State personnel have varying percentages of time to devote to this Project, and the Offeror must consider (and specify) time commitment expectations to the Project in creating the Project schedule and when obtaining information from State staff to create the above plans.

2.7. Utilize OIT's Document Sharing/Collaboration Capability

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

- Structure the document management and collaboration pages and data structures in such a manner as to support the overall requirements of the Project;

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

2.8. Project Management Methodology, Minimum Standards

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. Absent State direction to the contrary, all projects must include the minimum Milestones, Activities, Deliverables and Gates as specified below. For purposes of a summary project plan specific phase and gate dates, effort and costs are a sufficient minimum.

Following the award of this Contract, and during the project mobilization phase Contractors must include the following deliverables and milestones within their detailed project plans and methodologies at a minimum upon commencement of the project:

State Project Management Methodology, Minimum Standards

Phase	Milestone, Activity, Deliverable, Gate	
Concept Definition	Create Summary Plan	A
	Establish Key Milestones	D
	Establish Key Deliverables	A
	Establish High Level Project Plan	A
	Create Cost/Time Analysis (ROM)	A
	Establish High Level Dependencies	A
	Create High Level Project Schedule	D
<input type="checkbox"/>	Complete Gate 1 (G1)	G
Prioritization and Scheduling	Create Project Plan	D
	Identify / Secure Resources	A
	Create Detailed Cost/Time Analysis	A
	Create Phasing Strategy / Deliverables by Phase	D
	Initiate Procurement Activities/Plan	A
<input type="checkbox"/>	Complete Gate 2 (G2)	G
Requirements: Functional & Technical	Create/Maintain Project Plan	A
	Establish Implementation Strategy	D
	Create Stakeholder/Customer Communications Plan	A
	Create Detailed Resource Plan	A
	Establish Level 0 System Design	D
	Determine Existing Process Change Model	D
	Identify New/Enhanced Business Processes	D

	Finalize Implementation Strategy	M
	Finalize Development Tools and Production Requirements	A
<input type="checkbox"/>	Complete Gate 3 (G3)	G
Design: Functional & Technical	Follow/Track Final Project Plan	A
	Establish Final Cost & Time Estimate	M
	Create Detailed Design Documents - Functional	M
	Create Detailed Design Documents - Technical	M
	Establish Performance Requirements	D
	Establish Support Requirements	A
	Establish Operating Requirements	A
	Obtain System Application Software, Tools	A
	Create Process Flows with Key Inputs/Outputs	D
	Create Interface Control Documents	D
	Create Conversion/Migration Plan	D
	Create Integration Plan	D
	Develop Stakeholder Communications Materials	A
	Establish Technical Requirements	M
	Create Solution System Architecture Documents	D
	Update Enterprise Architecture Documents	A
	Create High Level Storage Requirements	A
	Create System(s) Sizing Requirements	A
	Establish Test Environment Plan	A
	Establish SDLC Environments	M
Brief/Update User Stakeholders/Customers	M	
<input type="checkbox"/>	Complete Gate 4 (G4)	G
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
	Complete Final Sizing Analysis	D
	Establish Operational Performance Baseline	M
	Publish Final Capacity Plan	A
	Prepare Component Test Analysis Report	D
	Develop Training Scripts	A
Develop Training Guide	A	
<input type="checkbox"/>		
Component Test	Establish Component Test Expected Results	D
	Establish Test Plan & Procedures	A
	Create Test Procedures	A
	Execute Component Test	M
	Collect Performance Metrics	A
	Produce Test Analysis Report	D
Create Component Technical Documentation	D	
<input type="checkbox"/>		
System Integration Test	Establish System Test Expected Results	A
	Establish Integration Test Expected Results	A
	Establish UAT Expected Results	A
	Establish Test Plan & Procedures	D
	Create System Test Procedures	A
	Collect Performance Metrics	A
	Produce System Test Report	M
	Create System Operational Documentation	D
Document/Publish Final Policies & Procedures	D	

	Publish Final Procedures	A
	Create System Technical Documentation	D
	Publish Version / Release Document	D
	Develop Training Scripts	A
	Develop Training Guide	A
<input type="checkbox"/>	Complete Gate 5 (G5)	G
(State) User Acceptance Testing	Support User Acceptance Test	M
	Document/Publish Issue/Bug List	A
	Prioritize Issues/Bugs	D
	Remediate Launch Critical Issues/Bugs	A
	Create Remediation Effort/Schedule for Outstanding Issues/Bugs	A
	Perform Final Performance Testing	M
	Create Operational Documents	D
	Create User Job Aids	A
	Update User Stakeholders / Communications	A
	Update Job Schedules and Dependencies	D
<input type="checkbox"/>	Complete Gate 6 (G6)	G
Production Deployment	Compile Release Checklist	D
	Transition Operational Procedures	M
	Publish Job/Control Schedule	A
	Assemble Audit Impact Statement (integrity, security, privacy)	A
	Create Release Verification Checklist	D
	Execute Operations Training	A
	Perform Release Verification	M
	Perform User Training	M
	Disseminate Documentation and Procedures	A
	<input type="checkbox"/>	Complete Gate 7 (G7)
Operate and Maintain (NOT IN SCOPE OF THIS RFP)	Establish Ongoing Operations Budget	A
	Establish Ongoing Enhancement/Development Budget	A
	Establish Ongoing Maintenance Budget	A
	Perform Break/Fix	A
	Establish Upgrade Plans	D
	Monitor Technical and Operational Performance against Operate Under SLAs	A
	Monitor Customer Adoption and Usage	A
	Market Services to Additional Customers	A
	Perform Operations	A
	Support Audit Functions	A
Remediate Audit Findings	D	
<input type="checkbox"/>	Complete Gate 8 (G8)	G

2.9. System and Acceptance Testing Requirements

For the solution technical implementation, code-based deliverables, development, upgrade / update or elements will be subject to a formal testing and acceptance process that uses objective and thorough test criteria established by the Parties that will allow the Parties to verify that each build meets the specified functional, technical and where appropriate, performance requirements. The testing and acceptance process will be developed for each build as soon as possible after establishing the business and user requirements. The testing and acceptance process will include sufficient audit trails and documentation as required to track and correct issues. The tasks and activities that the Contractor will perform as part of the testing and acceptance process include the following:

- Develop and maintain test data repositories as agreed appropriate;
- Develop test plans, scripts, cases and schedules as agreed appropriate;
- Perform the following testing activities for solution components and assess quality and completeness of results including:
 - Unit or Component Testing

- System Test / Assembly;
- Integration/interface testing and regression testing for new releases of existing applications; and
- Performance Test including regression testing new releases of existing applications as well as the potential performance impacts to current production environments where a risk of impacting performance may be introduced as a result of these elements;
- Provide test environments populated with quasi production data as required to perform the system and user acceptance testing work, and where appropriate performance testing. The test environments will be designed and maintained by Contractor so that test activities will not adversely affect the production environment. Contractor will expand capacity if testing requirements are constrain by the hardware;
- Perform technical architecture build/configuration testing (e.g. batch scheduling, interfaces, operations architecture, etc.); and
- ★ Document system and performance test results for State review and acceptance prior to the State's commencement of acceptance testing.

2.10. Performance and Reliability Testing Requirements

For any effort that involves the development of software code, custom configuration, scripts, batch processes, interfaces, data extractions, extensions to the system, changes/alterations (collectively Contractor Developed Elements) to Oracle provided data structures and the like, the Contractor will work with the State to develop an overall approach to performance testing of the impacted system elements as a result of the work described in this Supplement.

- ★ The Contractor will specify the appropriate performance testing approach that includes the design and execution of processes designed to demonstrate to the State that performance for any Contractor Developed Elements adheres to the agreed upon performance parameters and does not diminish the performance of the system beyond agreed values as a result of introducing the Contractor Developed Element into an production environment.
- ★ The Contractor will specify test environments as required to perform the appropriate performance testing. The test environments will be designed and maintained by Contractor so that test activities will not adversely affect the production environment. Contractor will expand capacity if testing requirements are constrained by the hardware.

The Contractor is to provide leading practices in conjunction with the overall performance 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, and regression testing of performance testing items.

2.11. System Changes as a Result of Contractor Activities

For those System Changes (updates, upgrades, patches or otherwise) to any State system or environment within the Contractor's scope of work that involve the change of code or data (provided system elements, software, Interfaces, Executables, Database Structures/Elements, operating system or database scripts, contractor developed code, interfaces, conversions, configuration items or otherwise) the Contractor will:

- Establish, publish and maintain a formal release calendar in consideration of the scheduled or required changes to the system;
- Develop release packaging rules that includes provisions for Contractor system and performance testing, State review and approval of Contractor results, provisions for State acceptance or validation testing (depending on the nature of the change);
- Operational procedures to backup or otherwise copy the system environment prior to implementing the change;

- Change implementation roles and responsibilities prior to making the change; and
- Rollback or reversibility considerations including success/failure criterion applicable to the change.

The Contractor will implement, utilize and maintain:

- State provided code management, version control tools based on the Rational change management suite or Contractor tools if mutually agreed with the State;
- Include requirements traceability for all elements of a system change;
- Ensure that all changes adhere to State security, privacy and data handling Policies as contained in Supplement 3;
- Employ standard test beds that are utilized and extended for purposes of fully demonstrating completeness of adherence to business, functional and technical requirements at State required quality levels;
- Utilize Contractor provided automated methods and tools for accomplishment of routine testing functions wherever possible; and
- If applicable, include performance testing for high volume (transaction or data) transactions at the mutual agreement of the State and Contractor in consideration of the contents of a change.

2.12. Project Solution Implementation Considerations and Requirements

The Contractor will complete full system implementation of the proposed solution to support the State’s focus on employee service for each user group (i.e., HRD and Agencies if applicable).

For asset based solutions (e.g., State hardware, licensed software and other elements are required to be purchased) the Contractor should propose and provide the technical architecture inclusive of hardware, software, networking requirements, implementation tools, integration tools, and reporting tools they recommend. The State is open to a modified technical architecture (operating system, etc.) for this new environments compared to the operating system/hardware configuration currently used by the State which is, in general predominately VMWare virtualized Windows Server based, Linux and selected popular Unix variants (e.g., AIX, Solaris, HPUX). The State assumes that all new environments required for this new installation of the Offeror proposed solution will be located at the State data center site for asset based (i.e., software hardware) from the start of the Project until it is migrated to the production environment or an alternative development environment provided by the State.

2.13. Project System Environments

The State requires that the following environments at a minimum will be provided and supported for the new installation of the Offeror proposed solution(s). The Offeror may propose any additional environments if they believe these environments are required to provide a fully functional solution based upon the Offeror’s approach.

- Development;
- System Test/Quality Assurance;
- Training; and
- Production.

The State believes the following phases will be required for the solution implementation. The Offeror may propose an alternate solution if they feel that it is in the best interest of State.

SDLC Phases	General Purpose
Mini-CRP	Conference Room Pilot where the solution requirements that were defined in the Design Phase are validated and gaps are documents. The Contractor will be required to stand-up a new solution Demo or Sandbox environment that will be used for the CRP.
Design	Design phase including but not limited to: <ul style="list-style-type: none"> ▪ Designs for any new reports; ▪ Designs for no more than 5 customizations;

SDLC Phases	General Purpose
	<ul style="list-style-type: none"> ▪ Configuration Workbooks; ▪ Security Design; ▪ Technical Architecture Designs; ▪ Operations Architecture Design; and ▪ Building of the Development environments.
Development	Development of any new reports and configurations, customizations, interfaces and reports. Unit testing of these development items. Build of security, technical architecture, operations architecture. Build of Testing environments.
Testing	System Testing. Integration Testing (including the CTI integration). User Acceptance Testing. Performance Testing (Contractor should recommend if this is required).
Deployment	End-to-End/Day in the Life Testing. Operations Readiness Planning.
Production	Rollout of the application to the user base.

2.14. Change Management/Communications and User Training

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

Change Management/Communications

- Contractor will work with the State to develop general communications materials regarding the scope, anticipated impact of change with regard to the change from existing methods to the Contractor solution(s). These communications documents must be focused (at a minimum) on general communique to all Agency HR State users;
- For State identified Agency HR Users, the Contractor will develop progress and design summaries to be shared by the State with these users;
- ★ For the HR Community function, HRD help desks that support Agencies and OIT help desks, the Contractor will develop targeted presentations that highlight specific system support processes, workflows, job aids and updates arising from the solution implementation

Service Delivery Functions User Training

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

It is the Contractor’s responsibility to establish and maintain data sets within each environment that are sufficient to support the training development and delivery requirements outlined above. As part of this activity set, the Contractor will:

- Document data set organization, integration across functions, location of source information, and any other information required to understand how data sets were built and conduct knowledge transfer to the State

2.15. Design Phase Responsibilities and Deliverables

The State has included in this RFP those deliverables which provide pertinent information to formulate a response. The following deliverables will be developed by the Contractor during the design phase:

- ★ Conceptual Designs and Validation
- ★ Enabling Technology Infrastructure Requirements and Conceptual Architecture
- ★ Enabling Technology Configuration and Operations Strategy
- ★ Enabling Technologies Business Technology Requirements
- ★ Conversion Approach and Design
- ★ Interface Approach and Design
- ★ Conference Room Pilot Scripts
- ★ Solution Updated Configuration and Operations Plan
- ★ Solution Business Technology Requirements
- ★ Conference Room Pilot Results

2.16. Construction Phase Responsibilities and Deliverables

The following deliverables will be developed by the Contractor during the construction phase:

The Contractor will be responsible for generating all code and configuration necessary to complete the technical implementation of the proposed solution. Contractor will, in its development, incorporate the use of coding and configuration standards, reviews, and requirements traceability, including release control. User walk-through(s) of the solution will be provided upon request. Contractor's efforts will include the creation and testing of test and production procedures and job schedules, as appropriate. Contractor will also perform the following tasks and activities in connection with implementing the proposed solution:

- ★ Establish, schedule and conduct design and build checkpoints with the State to review progress, code/system under development as to ensure that the final system meets State expectations and is acceptable to the State;
- Perform detailed technical design as agreed appropriate;
- Build solution components to support approved design specifications as follows:
 - ★ Configure, code and customize the solution requirements;
 - ★ Configure, code and customize solution interfaces;
 - ★ Configure and customize solution reports and forms;
- Design and Implement the security elements including user roles, permissions, IDs and other elements as required by the solution
- Build/configuration the technical architecture (e.g. batch scheduling, interfaces, operations architecture, etc.)
- Configure and customize integrated solution components and interfaces to external systems;
- Use technologically current development tools (e.g., development environments, code versioning tools, debuggers, compilers and user interface development toolsets) and languages as appropriate to improve programmer productivity, code stability and reusability;
- Perform unit test for solution components and assess quality and completeness of results;
- ★ Document solution and refine applicable acceptance criteria;
- Develop Applications in accordance with the State's strategies, principles, and standards relating to technical, data and Applications architectures as communicated to Contractor. Contractor will contribute to the ongoing development of such strategies, principles and standards through, at a minimum, advising the State of developments in technology which may be applicable to the State's business requirements;
- Conduct Build progress reviews with appropriate State personnel;

- ✳ Coordinate, confirm and provide the State approval of solution components and verification of applicable acceptance criteria for transition into Test activities.

2.17. Testing and Acceptance Phase Responsibilities and Deliverables

For the Offeror proposed solution implementation, any code-based deliverables and elements that are subject to a formal testing and acceptance process that uses objective and thorough test criteria established by the State and Contractor that will allow the verification that each build meets the specified functional, technical and where appropriate, performance requirements. The testing and acceptance process will be developed for each build as soon as possible after establishing the business and user requirements. The testing and acceptance process will include sufficient audit trails and documentation as required to track and correct issues. The tasks and activities that Contractor will perform as part of the testing and acceptance process includes the following:

- Develop and maintain test data repositories as agreed appropriate;
- ✳ Develop test plans, scripts, cases and schedules as agreed appropriate;
- Perform the following testing activities for solution components and assess quality and completeness of results including:
 - System Test / Assembly;
 - Integration/interface testing and regression testing new releases of existing applications; and
 - Performance Test including regression testing new releases of existing applications as well as the potential performance impacts to current production environments where a risk of impacting performance may be introduced as a result of these elements.
- Provide test environments as required to perform the system and user acceptance testing work, and where appropriate performance testing. The test environments will be designed and maintained by Contractor so that test activities will not adversely affect the production environment. Contractor will expand capacity if testing requirements are constrained by the hardware;
- Perform technical architecture build/configuration testing (e.g. batch scheduling, interfaces, operations architecture, etc.);
- ✳ Support the following testing activities relating to the State's performance of user acceptance test (UAT) for solution components as follows:
 - Develop with the State agreed upon UAT test plans, scripts, cases and applicable acceptance criteria.
 - Coordinate UAT execution and acceptance procedures with the appropriate the State participants.
 - Record and report UAT results.
 - Review changes, fixes and enhancements with the participants in the UAT testing.
 - Correct identified defects and nonconformities in accordance with the acceptance process.
- Compile and maintain solution issue lists;
- Conduct quality and progress reviews with appropriate the State personnel;
- Coordinate and confirm the State approval of solution components and verification of applicable acceptance criteria for transition into deployment and production use; and
- Production Implementation Phase Deliverables.

2.18. Pre-Production/Production Deployment Phase Responsibilities and Deliverables

Contractor will be responsible for working with the State and its third party contractors, and executing the production deployment and roll-out of the solution to the Production Environment.

If the Deployment includes software deployment to the End User Desktop Equipment or file server elements (if applicable), 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.

Contractor will comply with the State required implementation and deployment procedures. This may include, network laboratory testing, migration procedures, the use of any pre-production or pseudo-production environment prior to production migration. Contractor will be responsible for business user support required during the initial weeks of a production deployment as determined by the affected State business units and will maintain the capability to provide enhanced levels of support during the term of the project.

- ★ Contractor will submit to the State, for the State's approval, a written deployment plan describing Contractor's plan to manage each such implementation, including working with the State's OIT infrastructure team, if applicable. The tasks and activities to be performed by Contractor as part of the this phase also include the following:
 - Execute required data conversions and migrations including, but not limited to, baseline system configuration tables and parameters, and ancillary supporting data as required by the system to function successfully in the production environment:
 - Establish data to be used with the new solution by producing new data and reconciling and mapping different data and database representations.
 - If required, convert electronic data into a format to be used by the new solution using the data conversion program.
 - Perform required data matching activities and error reporting.
 - Document data issues and provide to the State for resolution.
 - Coordinate and confirm the State approval of data conversion results.
 - Conduct production pilot(s) (including "day in the life" simulations) and fine tune solution as agreed appropriate;
 - Compile and maintain solution issue lists;
 - End to end final validation of the operational architecture for each solution area (i.e., HRD, Agency HR and others as applicable)
 - Conduct quality and progress reviews with appropriate State personnel;
 - Develop, and thereafter make available to the State, a knowledge base of documentation gathered throughout the Project's life and allow for re-use of such documentation for future Projects; and
 - Transition solution support responsibility to the State.
- ★ Conduct a post-implementation review process upon the completion of the Project which will include an analysis of how the business system(s) resulting from the Project compare to the post-deployment performance requirements established for such Project.
- ★ Establish a performance baseline for the Project business systems, and where appropriate document requirements for future performance enhancement of the business systems implemented as part of the Project.

2.19. Post Implementation Support Responsibilities and Deliverables

For a period of no less than ninety (90) days unless otherwise agreed by the State, and in consideration of Service Levels then in effect, Contractor will provide sufficient staffing to ensure the overall continuity of the solution as it pertains to delivering these services in a production environment either operated by the State.

In the event that a Priority 1 or 2 issue (or any critical blocking issue, as defined in Sections 7.9.1 and 7.9.2) occurs during this 90 day period, this 90 day period may be extended at the sole discretion of the State for a period commencing upon satisfactory resolution of the issue in the production environment. Under no circumstances will the Contractor performance during this period, successful conclusion of this period (i.e., no issues detected for 90 days) be construed as relief from or reduction to any Software Warranty considerations contained in this RFP.

During this period the Contractor must:

- Provide personnel with the requisite skills and experience levels in development of the solution to answer questions that the State or Hosted Services Provider may have;

- Address any software defects, gaps, omissions or errors that are discovered in the Contractor's work as they pertain to operation in a production environment;
- Resolve any configuration, performance, compatibility or configuration issues that arise as a result of migration of the Contractor's work to a production environment;
- Document any relevant changes to operational, configuration, training, installation, commentary or other documentation as a result of migration to the Contractor's work to a production environment; and
- Assist either the State or Managed Services provider with production issue triage, root cause and remedy analysis and wherever possible propose workarounds, fixes, patches or remedies (code-based, procedural or environmental) required to successfully transfer and operate the Contractor's work to a production environment.

3.0 HRD Document Imaging Requirements

3.1 Objectives and Overview

The Department of Administrative Services (DAS) Human Resource Division (HRD) is seeking a Document Management System (DMS) to enable both HRD and Agency Human Resource Departments the ability to streamline document management functionality, aggregate key sources of personnel documents to one official repository of record, manage the retention of documents, and empower Human Resource personnel to focus on core services to their customers. Key objectives of the DMS are:

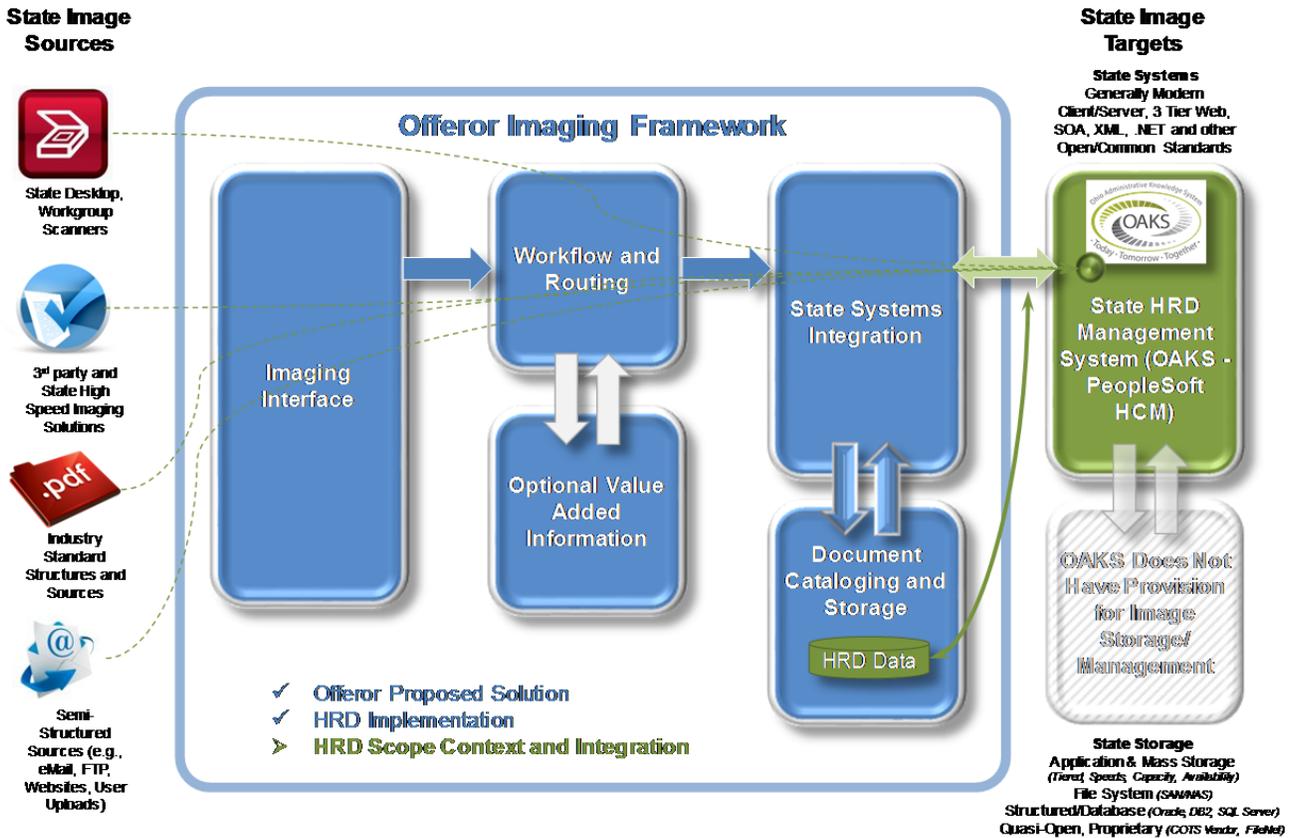
- To migrate and index all Human Resource Division (HRD) electronic documents from the current FileNET System.
- To capture, index, store, and retrieve HR Personnel Documents still being delivered from other agencies to HRD.
- To migrate and index all completed ePAR (Electronic Personnel Action Requests) with attachments and ePerformance (Performance Evaluations) with attachments from the Ohio Administrative Knowledge system (OAKS) Human Capital Management System (HCM) (including support documents) into the new DMS System.
- To import on a regular basis employee Personnel Action documents and attachments created from ePAR (System within OAKS HCM Systems to their respective destination in the DMS system.
- To import on a regular basis ePerformance and attachments from the OAKS HCM System to their respective destination in the DMS system.
- To enable other agency Human Resource departments to deploy the full capabilities of the DMS system to capture, index, store, and retrieve all their HR personnel documentation.
- To deploy dynamic retention rules to manage the disposition of employee personnel records based on State of Ohio policies.

Other objectives include:

- Reduce storage, printing, filing, faxing, and mailing costs along with creating a central repository for key documents within Agency Human Resources departments.
- Provide separate secure file for confidential medical information.
- To provide common administrative functions state-wide that allow agencies to focus on their core missions.
- Provide a standard method for processing documents with image legibility and valid metadata.
- Centralize the storage of electronic documents and scanned document images and provide a consistent user experience for retrieving documents.
- Ensure integrity and continuity of record keeping.
- Ease of use for HRD and participating agencies.
- Provide a mechanism to identify and purge inactive records which is expandable and flexible enough to meet agency specific needs.
- Standardize the procedures for disposal of obsolete records.
- Increase compliance with legal and audit retention requirements.
- Allow for the fulfill Public Request for Records that may require redaction and selection.
- Reduce support and operating costs by consolidating multiple DMS platforms used by various agencies into one common DMS platform.

3.2 Context Diagram: HRD Requirements and Overall Enterprise Framework

Using the Enterprise Framework Diagram from Section 1.2, the context of the HRD implementation using a conceptual framework is as follows:



Offerors are to note that the HRD function in the State utilizes OAKS (based on PeopleSoft HCM) as its system of record for all HR transactions including Payroll, Benefits and Performance Management among other functions. OAKS is not designed for, nor has provision for the incorporation, cataloging and storage of images, therefore the solution proposed should maintain these images outside of OAKS and provide mechanism(s) to reference or use the imaged alongside of OAKS as a support function.

3.3. Organizational Overview

Department of Administrative Services (DAS)

The Ohio Department of Administrative Services (DAS), is committed to providing quality centralized services, specialized support and innovative solutions to state agencies, boards and commissions. DAS has more than 40 program areas serving Ohio government customers, who in turn directly serve the interests of Ohio citizens. DAS helps procure goods and services, deliver information technology and mail, recruit and train personnel, promote equal access to the state workforce, lease and manage office space, process payroll, and print publications and perform a variety of other services. To provide these services, DAS is organized into the divisions of Equal Opportunity, General Services, and Human Resources as well as the Office of Collective Bargaining and Office of Information Technology.

About the DAS Human Resources Division (HRD)

The Human Resources Division, within the Ohio Department of Administrative Services, performs a variety of functions including overall support of the state's human resources operations for state employees. This division provides services and information to state employees and assists state agencies in conducting their human resource functions. Services are offered in the areas of policy development, payroll administration, benefits administration, classification and compensation, drug testing, central recruiting, training and development, workforce planning and records maintenance.

HRD HR Operations

This office is responsible for all functions supported by the Ohio Administrative Knowledge System (OAKS), Human Capital Management (HCM) module and for providing direct assistance to agency HR, Benefits and Payroll

staff; including; personnel action processing, certification lists, statewide employee records, time and labor, state payroll processing and statewide benefits processing. The office also serves as front-line support for all customers of the OAKS HCM module.

HR Operations, State Personnel Records

The State Personnel Records unit is a part of HR Operations. Responsibilities of the State Personnel Records unit include maintenance and archiving of records that documents an employee’s history of employment with the State and maintenance and archiving of position descriptions.

A primary task of Records is to ensure access to former and current employee records to satisfy the needs of Public Request for Records. Typically, this function requires documents to be captured, indexed, stored, retrieved, and redacted. While Agency Human Resource departments create and manage all their relevant employee records, the State Personnel Records department will only store and manage a subset of these documents.

Agency Human Resource Departments

At the agency level, Human Resource departments create a variety of document types throughout the lifecycle of an employee. From the employee on boarding process to separation an Agency HR Department will include but not limited to the following document types:

- Benefits,
- Disability,
- Disciplinary actions,
- Education and Commendations,
- Medical records,
- Orientation (New Hire),
- Performance Evaluations,
- Position Descriptions (PD), and
- Personnel Actions (PA).

3.4. Required Implementation Timelines

Offerors are to include the following major phase completion milestone requirements as part of their response. Offerors may propose shorter delivery dates as long as State technical, functional, cost, risk, participation and quality considerations are not compromised:

- Complete and deploy phases 1 and 2 of the proposed Imaging system rollout to production status no later than June 2015.

3.5. State Personnel Record, Logical Mapping, Hierarchy and Data Elements

Below is a table of the logical fields, relationships and hierarchy information for personnel records that is designed to assist Offerors in developing their response to this RFP as well as to be included for development, conversion and integration purposes as applicable. This document is for illustrative purposes.

	Employee Records Document Hierarchy	Transfer w/employee	Agency Access	HRD Access	HCM Interface
0.0.0	AGENCY Name				
1.0.0	Folder 1: Personnel Actions (with Attachments)				
	Hire-Rehire- up to 25 Document types	No	Yes	Yes	Yes
	Data Change Current Employee- up to 75 Document Types	No	Yes	Yes	Yes

	Discipline- up to 10 Document Types	No	Yes	No	Yes
	Termination- up to 30 Document Types	No	Yes	Yes	Yes
2.0.0	Folder 2: Administrative				
	Up to 20 Document Types	Yes or No depending on the document	Yes	Yes or No depending on the document	Yes or No depending on the document
3.0.0	Folder 3: Payroll and Benefits				
	Up to 15 Document Types	Yes or No depending on the document	Yes	No	No
4.0.0	Folder 4: FMLA/Medical				
	Up to 40 Document Types	No	Yes	No	No

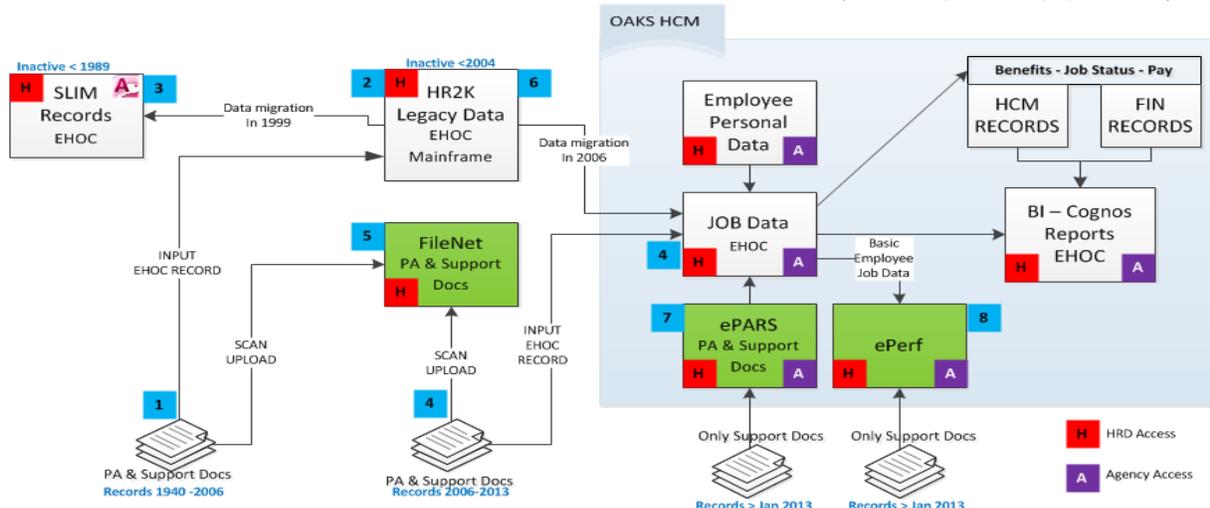
3.6. Current State HR Operations State Personnel Records Unit

The State Personnel Records unit is responsible for fulfilling Public Requests for records which requires a file search, retrieval, and sometimes redaction of sensitive data. Today, multiple systems are accessed to retrieve the Personnel Action forms, relevant supporting documents, and Employee History on Computer (EHOC) data for an employee record. Historical EHOC files are accessed from MS Access SLIM Records and HR2K mainframe, while current EHOC records are access from OAKS HCM System. At this time EHOC records are out of scope for this project.

3.7. Architecture Overview and Volumetric Information: Current HRD Personnel Records Systems

DAS HRD Personnel Action Documents – Current State (9/25/2013)

- A) FileNet system contains 2.7 million documents with 8.6 million pages.
- B) HR2K System has 25 million EHOC records
- C) ePARS is supported by SmartERP (Oracle Module). Contains 17,000 PA Records. Support documents are attached in native format. Word, Excel, jpg, tiff, bitmap.
- D) ePerformance supported by PeopleSoft (Oracle Module). Contains 13,000 records / 4,000 are complete.



- 1) From 1940-2013 PA/Docs inputted into FileNet.
- 2) PA data stored in HR2K until 2006.
- 3) In 1999 a portion of HR2K data was migrated to MS Access DB – called SLIM Records. Used today for Public Request for Records.
- 4) In 2006 OAKS went live. PA data inputted into JOB DATA which directly affected employee pay, benefits, job status.
- 5) PA/Docs still captured into FileNet

- 6) EHOCS data for all Current employees and Inactive employees from 2004 migrated from HR2K to JOB DATA. Inactive employees from 1990-2004 maintained on HR2K. Inactive employees <1990 maintained on MS Access.
- 7) In Jan 2013 most agencies use ePARS to submit electronic PA/Docs. Paper copy still maintained at agency level. ePARS is not a official repository of record. Other agencies still submit paper PA/Docs.
- 8) In Jan 2013 ePerformance used by agencies to create and manage performance evaluations. Only used by agencies and not by HRD.

3.8. HRD State Personnel Records Repositories

From the HRD HR Records Perspective, there are two repositories that maintain employee personnel records (1) ePAR and (2) FileNET, each will be presented in turn.

ePAR (Electronic Personnel Action Request) System – a module on the OAKS Human Capital Management (HCM) System contains PDF documents beginning in January 2013.

Beginning in January 2013, HRD initiated the ePAR (Electronic Personnel Action Request) System to automate the Personal Action form process. It is a module within the Oracle OAKS HCM environment. Agencies can now complete the entire Personnel Action process online through an automated workflow process. Once the PA is completed it directly engages the JOB DATA file within the OAKS HCM application to execute the change in employee's pay, benefits, or job status.

- ePAR is supported by SmartERP (Oracle Module):
 - Contains 17,000 PA Records.
 - Support documents are attached in native format. Word, Excel, jpg, tiff, bitmap.
 - Records are retrieved by the employee's State of Ohio ID Number and not by a SSN.
 - Since ePAR is not considered the repository of record for records, agencies are required to print and file the PA document in their employee's personnel file.
 - Records are retrieved by the employee's State of Ohio ID Number. There is no SSN associated to the record.
- ePAR conventions:
 - Once an ePAR has been completed and finalized it cannot be modified.
 - If the ePAR is incorrect and deleted from the HCM System, then the ePAR version in the DMS must be manually deleted too.
 - If a completed and finalized ePAR adds a new support document, the ePAR system will insert a creation date. The system will then migrate the new document into the DMS.

FileNET System v4.1

Before ePAR was implemented in January 2013, all agencies under the jurisdiction of DAS submitted their Personnel Action Forms and Support Documents to be captured, indexed and uploaded into FileNET System. Agencies submit finalized Position Descriptions (PD) to be captured, indexed and uploaded into the FileNET system. Approximately 2.6 Million documents with 10.6 Million pages have been captured into the system.

- System contains scanned copies of PA forms from 1940-2013.
- Allows files to be layered for Redaction.
- While most agencies have migrated to using ePAR, a few agencies are still submitting paper PA documents that need to be captured and indexed.
- Supported by IBM.
- FileNET has limited usage within the enterprise.
- FileNET requires separate sign-in to Capture docs and retrieve docs.
- All PA plus supporting docs are scanned together as one document.

FileNET Personnel Action (PA) Process and Support Requirements:

- PA plus support documents are scanned.
- Scanned documents are indexed with SSN, Employee ID number, Employee Name, Effective Date, type of PA or document.
- Combined into the FileNET system.

- The stack of packets consisting of PA's and attachments from Agencies are obtained from the inbound drawer and scanned into the FileNET client application.
- HR Records technicians then begin their process of proofing the scanned PA's, processing and indexing the metadata to incorporate the information into the FileNET Client Application.
- A process verifies the content entered into FileNET and if necessary, the HR Records Technician utilizes OAKS (looking for name, employee ID or social security number and other personal information discrepancies), then incorporates the metadata and document into FileNET.
- Search – typically search by Employee ID, SSN, name, Action, and Effective Date.
- Records requested are redacted in FileNET but original version is not altered. Key data is blocked out.

FileNET Position Description (PD) Process and Support Requirements:

- PD is scanned.
- Scanned document is indexed with Position Number, Effective Date, Agency ID and PD Type
- The stack of PD's from Agencies are obtained from the inbound drawer, processed, and scanned into the FileNET client application.
- HR Records technicians then begin their process of proofing the scanned PD's, processing and indexing the metadata to incorporate the information into the FileNET Client Application.
- A process then incorporates the metadata and document into FileNET repository.
- Search – typically search by Position Number.

3.9. HRD Users and General Responsibilities

Following are the different types of HRD State Records user(s) who participate in processing HR Records:

User Type	Responsibilities
HR Records Manager	Management of DAS – HR Records department including <ul style="list-style-type: none"> ▪ Retrieval of employee records and documentation ▪ Processing legible content and maintaining accurate records retention ▪ Managing requests from Agencies, Public, and Media outlets
HR Records Technician	<ul style="list-style-type: none"> ▪ Preparing documents ▪ Scanning documents ▪ PA proofing ▪ Indexing and metadata tagging for employee records maintenance and ▪ Ongoing archival ▪ Retrieving documents to fulfill record request
HCM State Services Analyst	<ul style="list-style-type: none"> ▪ Process PA's

The following is a listing of companion and common software used in the HR records process:

Software	Description
Adobe	PDF Creator used for personnel records are requested to represent the personnel records (with the appropriate information redacted to comply with Ohio law)
EHOC	Employee History on Computer
FileNET Client Application	Used for adding index data & correcting indexed data per OAKS. The application is a permanent repository of PA's
OAKS	Ohio Administrative Knowledge System developed using PeopleSoft V9.1 for various departments to perform respective tasks. HR Records uses this for searching employee information and verifying FileNET metadata

The following is representative of typical hardware used to process HR Records:

Hardware	Description
Client Machine	Configuration: Operating System – Windows XP (SP3), Windows7 Pentium @ D CPU 2.80 GHZ, 2,79 GHZ, 0.99 GB RAM Dual Monitors
Scanner	Bell Howell Copiscan 8000 Plus

3.10. Current State – Agency Human Resource Departments

Human Resource Departments within all State agencies, boards, and commissions create and manage all employee personnel records including the executions of all Personnel Action forms to modify pay, benefits, and job status.

There are two types of methods agencies use to manage their HR documentation:

- **All Paper Environment** – Agencies create and manage all Human Resource employee personnel records in paper. Paper documents are stored in traditional folders and filing cabinets. Inactive records are maintained for a stated period of time until they are transferred to the State Archived repository.
- **Document Management System Environment** – Many agencies have deployed Document Management Systems for their HR Department, and for some, the entire agency itself. Whereby all personnel documents are stored and managed within the system. Common DMS platforms include Hyland OnBase, Intellinetics, FileNET, and SharePoint.

Regardless of the environment, agencies are using the ePAR system (similar to DAS HRD) to create and approve their Personnel Actions. Since ePAR is not the official repository of records, agencies are required to store the ePAR within their own paper folders or DMS system. Once an ePAR has been approved and completed the system creates a PDF copy with attached supporting documents. For agencies with a DMS system, the ePAR must be manually captured and indexed. For agencies using paper storage, the ePAR must be printed and filed into the employee folder.

Agencies are now required to use ePerformance to create and manage their employee performance evaluations. Once an ePerformance evaluation has been approved and completed, the user will manually create a PDF copy with attached supporting documents. For agencies with a DMS system, the ePerformance evaluation must be manually captured and indexed. For agencies using paper storage, the ePerformance evaluation must be printed and filed into the employee folder.

ePerformance System Information (Agency related only)

- Supported by PeopleSoft located within the Oracle OAKS HCM Environment.
- January 2013 HRD initiated the ePerformance application which is a module within the Oracle OAKS HCM environment. Integrated to the OAKS HCM platform, ePerformance is a web based application that facilitates the workflow process to create and manage employee performance evaluations.
- ePerformance streamlines the appraisal aspect of the development business process, from goal planning and coaching to performance assessments.
- Managers, employees, and HR administrators can collaborate on performance evaluations and goals, review performance history, and monitor and manage the overall performance process.
- Workflow notifications keep all interested parties up-to-date throughout the performance cycle.
- The purpose of ePerformance is to provide an enterprise solution for all employee performance evaluations, Performance Improvement Plans, and Career Development Plans. It allows the State to oversee the management, utilization, and proliferation of the program down to agency levels.
- As of August 2013 there are 12,300 ePerformance Documents in the system.
- 4,000 documents or evaluations have been completed.

- Supervisors can create and update a current document.
- All completed documents are read only.
- Supervisor has a copy for his records.
- The Employee's record will be part of their historical documents indefinitely.
- A DAS Program Administrator is the only person who can delete records permanently.
- Documents can be canceled. The documents will still exist in the system but no longer be accessible to the employee.
- Documents can be reassigned.
- Document in process can be reassigned to new supervisor.
- Completed documents always remain with supervisor who signed it.
- Business Intelligence (BI) – uses Cubed Data on Personnel data.
- ePerformance record handling requirements.
- Once an ePerformance document is completed and finalized it cannot be modified.
- Once an ePerformance document is completed and finalized the ePerformance system cannot add another support document.

3.11. General HRD System Requirements

At a minimum, Personnel Action records and support documents in FileNET and ePAR Systems need to be combined into the proposed DMS system for HRD and agencies to access.

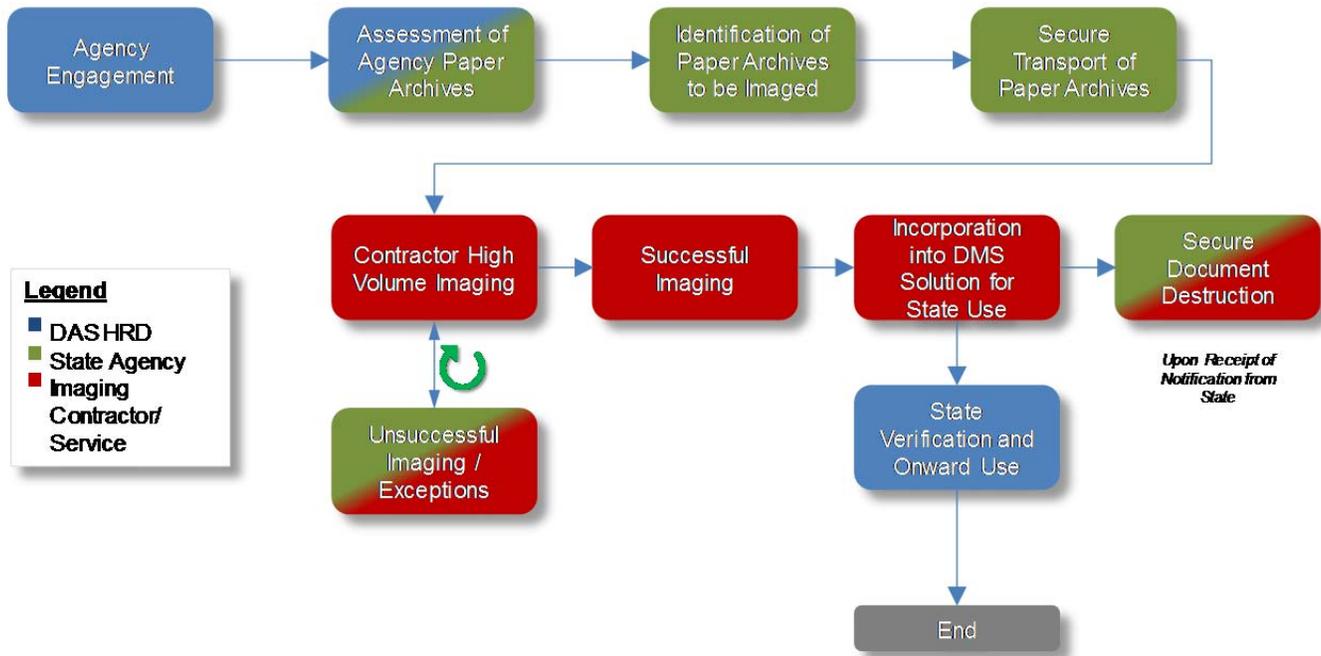
Relevant employee records for HRD from separate systems need to be combined into the proposed DMS system including:

- Personnel Action and support documents in FileNET System (Required).
- Personnel Action and support documents in ePAR (Required).
- Automated OCR and indexing.
- Workflows should be easily modifiable without the need for specialized training or certification.
- The State (with appropriate training) shall have access to the full capabilities of the system without the need for contractor or systems integration specialist skills,
- The system shall provide for enterprise level licensing as opposed to agency by agency user groups or pools
- Automated or assisted redaction technology.

3.12. High Volume Offsite Imaging Services Requirements

As mentioned elsewhere in this Supplement, the State maintains a variety of HRD and Agency specific paper archives that may be required to be imaged and migrated to the Offeror provided solution. In general the volume and extent of these paper archives will vary based on project phases (contained herein) or as additional Agencies are engaged to adopt the enterprise HRD Imaging Solution. As a result of this adoption, the State may have requirements to process these paper archives as follows:

General High Volume Imaging Process Flow (Paper Based Conversions)



In general, this process is as follows:

- The process will commence with DAS HRD engaging an Agency (either within the scope of phases described in this Supplement or for Agencies beyond its scope) and collaborate with the Agency to determine what (if any) paper based records would be beneficial to the State and Agency for inclusion in the imaging system;
- Following the determination, and based on cost/benefit and other practicalities, the State Agency may transport these paper records to the Contractor (or Sub-Contracted Service) location for imaging and incorporation into the HR system;
- The Agency may have to collaborate or support the Contractor in addressing issues and exceptions for certain documents and support scan/not-scan decisions based on these issues/exceptions; and
- Following State verification that the documents are incorporated into the imaging solution, the State may direct the Contractor to securely destroy the paper based documents.

As part of the response to this Supplement, the Offeror will demonstrate its understanding of these processes and service requirements and illustrate their ability to support the State using the proposed system. In addition, Offerors are instructed to include a “per image” cost for these circumstances in the Offeror Cost Proposal form for this RFP.

3.13. Agency HR Department General Requirements

- The ability to migrate and integrate ePAR and ePerformance into agency systems and processes. In a typical week, an agency can create and manage hundreds of Personnel Action documents.
- For agencies with or without an existing DMS Systems the automated capture and index of ePAR and ePerformance documents while reducing labor intensive processes and indexing error exposure.
- The ability to migrate and integration of ePAR documents into the proposed system to save time while facilitating more effective and extensive search capabilities for managing and accessing documents.
- The elimination of filing, duplication and retrieval costs of off-site paper storage.

- To accelerate the process to fulfill Public Records for Request and to redact personal information as required.
- The ability to share and distribute documents seamlessly through email, fax or State systems.
- The ability to access documents from remote locations via the internet or State private networks.
- Maintain consistent role based accessibility rules with security, assisting users in retaining strict control over which documents are available to staff and the general public under the provisions of Ohio law and Supplement 3 pertaining to data handling and security.
- Secure backup of files and records for disaster recovery purposes on State or Contractor provided storage media.
- Maintain and manage review, processing and approval queues for documents that must be viewed and signed by other personnel.
- To minimize the State's exposure for lost documents, once documents are presented or introduced to the system environment, a clear traceability of all documents accepted, rejected, advanced, filed, processed, archived, deleted/removed or forwarded to a State system for storage must be maintained.
- The system must provide intelligent search methods that support searching with a variety of intuitive criteria including diacritic, soundex, name, date, form type and other methods to minimize search time and maximize efficiency of State personnel.

The Contractor's implementation project for the Document Management System inclusive of design, implementation, testing and deployment phases must enable both HRD and participating agencies to:

- Migrate and index all HRD FileNET Documents for HRD usage only.
- Migrate and Index all existing completed ePAR and supporting documents.
- Identify new support documents for a completed ePAR and migrate and index it into the system.
- Import and index on a regular basis all completed ePAR and supporting documents.
- Migrate and index all existing completed ePerformance and supporting documents.
- Import and index on a regular basis all completed ePerformance and supporting documents.
- Migrate and Index all documents and records from an existing Agency DMS system into the new system.
- Provide automated retention rules to assigned documents.
- Use OIT's Microsoft Active Directory (ID Domain) to authenticate user logins.

3.14. Agency Migration Requirements

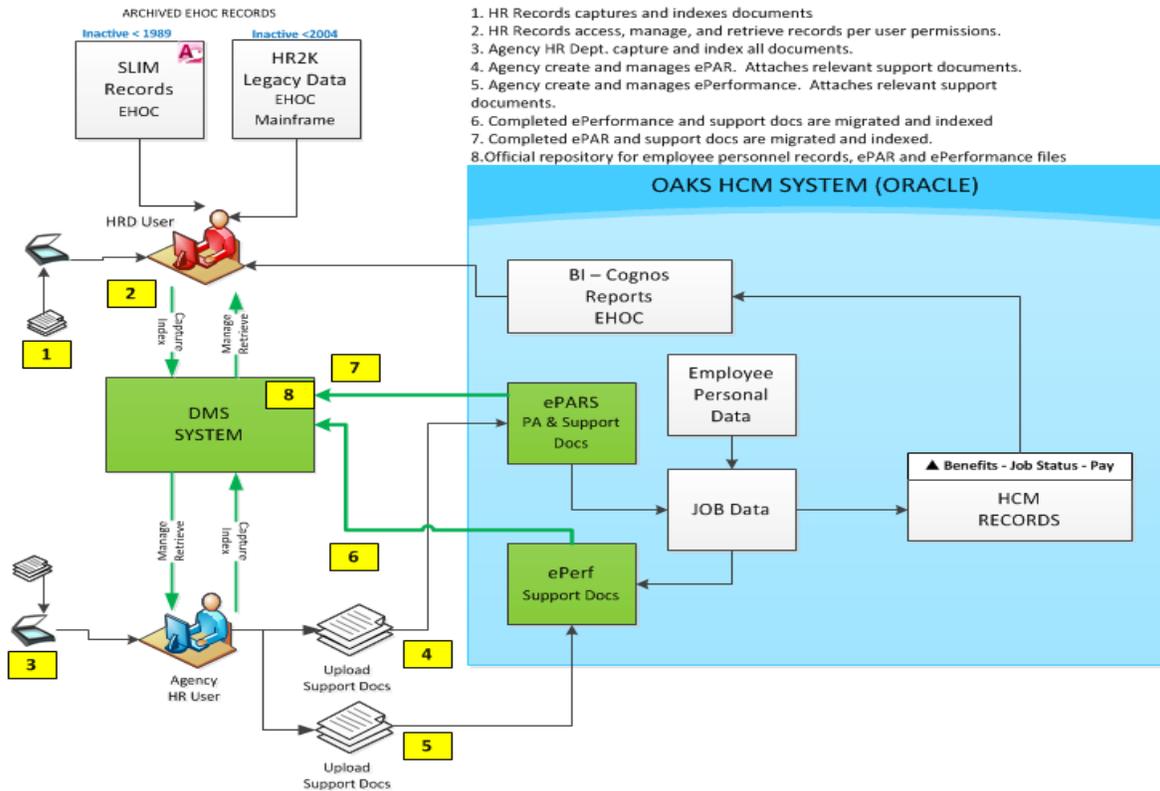
The DMS platform will be available for all State agency Human Resource departments to either (A) Deploy from their paper environment, or (B) Migrate from their existing DMS platform to the proposed system. Agency HR Departments must have access to the full capabilities of the DMS to capture, manage, and retrieve all their personnel records, including the disposition of records according to their retention policies. The document management solution will be accessible based on industry standard security protocols to HRD and participating State agencies.

The system will be scalable to meet the demands of multiple agencies and their users while accepting the majority of document types including performance evaluations and discipline files. While HRD functions are the initial implementation scope of this RFP, the State envisions this platform serving as a potential basis for an enterprise imaging framework. Therefore, the system will have the provision for the separation of secure and encryption of confidential medical, citizen (HIPPA/PII) information.

3.15. DMS Integration Diagram

The following diagram is designed to illustrate the State's integration requirements for the Offeror proposed system. These integrations include:

- Integrations/Conversions from legacy State image and HR data stores (i.e., SLIM and HR2K);
- Integrations/Conversions from existing HRD image stores;
- Integrations/Conversions from existing Agency imaging functions;
- Integrations to OAKS HCM;
- Logical orientation context of ePARS and ePerf processes, workflows and data; and
- High level indication of process flow, image sources and the general context for the operating and integration environment for the Offeror proposed solution.



3.16. Required Operating Environment and OAKS Integrations

The HRD Document Management System will be designed and implemented to serve as the official repository of Record for State of Ohio employees Personnel Records and supporting documents. By using the full capabilities of the DMS system, HRD will manage and retrieve all relevant Personnel Records and supporting documents migrated from the FileNET system, ePAR, and manually submitted documents.

The Ohio Administrative Knowledge System (OAKS) is the State's Financial and HR/Payroll/Benefits management system which is based on PeopleSoft HCM v9.2.

On a scheduled, near real time batch basis, the DMS system will import ePAR and ePerformance files from the HCM OAKS Environment, index and route them to their respective owners, thus making the DMS system an official repository for employee personnel records. As part of this process the proposed system will associate Social Security Numbers, State Employee IDs, and employee names to ePAR and ePerformance documents to facilitate HR Records lookup. When a completed ePAR and/or ePerformance document has been imported into the system, the system must be able to recognize and import support documents that have been added afterwards to ensure the Official Record is complete. Following this process, ePAR and ePerformance documents will be accessible based on user roles and permissions.

3.17. DMS Usage Scenarios by HRD and Agencies

As part of their response, and to assist the State in understanding the capabilities, merits, features and possible limitations of the Offeror proposed solution. Offerors will provide (based on the data contained in this RFP and Offeror experiences in implementing the proposed solution) narrative and illustrations for the following Document Management System Usage Scenarios:

1) Use of the DMS system to migrate FileNET Documents, ePAR and ePerformance documents.

- Overall Approach and Process Description.
- Cost and Cost Drivers (e.g., sources, complexity, volumes) to import and index documents into DMS System.
- Cost and Cost Drivers to import ePAR and ePerformance documents, including indexing and mapping to destination folder.
- Other considerations that highlight the merits of the proposed solution and drivers of unanticipated costs.

2) Agency Human Resource Department conversions from paper based filing systems.

- Cost and Cost Drivers (e.g., sources, complexity, volumes) Cost to have provider capture and index documents.
- Determining factors and considerations regarding Agency purchases of high end scanning devices to capture and index their documents vs. desktop scanners or contracted scanning services to capture and index paper based documents.
- Other considerations that highlight the merits of the proposed solution and drivers of unanticipated costs.

3) Conversion of existing Agency Human Resource Departments with pre-existing DMS systems

- Cost and Cost Drivers (e.g., sources, complexity, volumes) Cost to import and index documents to new system from existing system(s) that are a) based on the Contractor proposed system or b) .based on alternative solutions.
- Other considerations that highlight the merits of the proposed solution and drivers of unanticipated costs.

3.18. Requirements and Sizing: Document Migration from Existing DMS Platforms

Offerors will propose and execute the following conversions as part of the project. Volumetric/sizing data is provided to assist Offerors in determining costs and relative scope. While this table includes some data that is out of scope (i.e., SLIM and HR2K) the Offeror should offer an approach and conversion considerations for the State in its response. Based on the relative effort and cost, the State may elect at a future date to include these conversions under an authorized change order to any contract arising from this RFP.

HRD Systems					
Agency	Migrate	Platform	Documents	Pages	HR Users
HRD	Yes	FileNET Docs	2,635,173	10,644,887	15
HRD	Yes	HCM Docs	30,000 Records	Need to add attachments	5

Other State Agency Systems (examples)					
Agency	Migrate	Platform	Documents	Pages	HR Users
DVS	No	Hyland OnBase	1,596,375 (55 GB)		38
BWC	No	SharePoint 2007	~1,000,000		30
Medicaid	Yes	FileNET Version IBM P8 V5.1	544 records	Average 233 pages per employee or 126,752 pages	12

Migrating Agencies with Paper Based Processes					
Agency	Inactive Documents	Active Documents	Weekly Document Volume	Image Sources	Users
DAS	160,000	92,000	700	Multi-functional copier scanner	13
AGR	65,000	40,000	500	1 - A networked Konica Minolta Bizhub Copier, Fax, Scanner	8
DODD	90,000	36,000	6,000	Has Multifunction a copier/scanner Has dedicated high speed scanner; a Kodak, i1420	50
GOV	n/a	10,000	50	None	2
OOD	n/a	50,000	500	None	19

3.19. HRD Imaging Requirements Matrix

The State has developed a set of functional requirements contained in the next section of this supplement pertaining to HRD solution needs. To assist the State in reviewing the Offeror’s response, the Offeror proposed solution or tools in satisfying these requirements and understand the implementation scope, approach and dependencies that will be in effect for the implementation and ongoing operation and maintenance of the Offeror solution, Offerors will complete the Requirements Matrix as follows:

- Offeror Proposed Tool/Solution** Offerors are to include the name and major version number of the Proposed Tool/Solution to address the requirement (e.g., Acme Corporation® WidgetMaster™ v9.1).
- Out of the Box** Offerors are to indicate, in full lifecycle development hours (i.e., design, implement, test), the number of hours to be spent implementing this requirement using as delivered functions of the Offeror proposed solution. Should this not be applicable, Offerors are to record a zero (0) in this column.
- Configuration Item** Offerors are to indicate, in full lifecycle development hours (i.e., design, implement, test), the number of hours to be spent implementing this requirement using as configurable functions (e.g., interfaces, reports, workflows, screen elements) of the Offeror proposed solution. Should this not be applicable, Offerors are to record a zero (0) in this column.
- Customization** Offerors are to indicate, in full lifecycle development hours (i.e., design, implement, test), the number of hours to be spent implementing this requirement using as configurable functions (e.g., interfaces, reports, workflows, screen elements) of the Offeror proposed solution. Should this not be applicable, Offerors are to record a zero (0) in this column.
- Extension/Interface** Offerors are to indicate, in full lifecycle development hours (i.e., design, implement, test), the number of hours to be spent implementing this requirement using as extensions or interfaces (e.g., interfaces, reports, workflows, screen elements) of the Offeror proposed solution to OAKS (PeopleSoft), State CTI interfaces, or other Offeror provided solution elements. Should this not be applicable, Offerors are to record a zero (0) in this column.
- Other** Offerors are to indicate, in full lifecycle development hours (i.e., design, implement, test), the number of hours to be spent implementing this requirement using as that do not fit into the aforementioned categories. Should this not be applicable, Offerors are to record a zero (0) in this

column.

For the avoidance of doubt, all Offeror proposed hours for the effort, absent Project Management and Client administration and production migration associated with compliance with State requirements must be included in the provided Requirements Matrix.

3.20. HRD Solution Requirements Matrix

The following is the listing of HRD solution requirements in their entirety. The State has prioritized the functional requirements based on current need as follows:

- 1 - Required** Mandatory requirements that the Contractor must include in their proposal, design, implement and test and support the production use of in their response

- 2 - Preferred** Requirements that the State believes are dependent on implementation of Must Have requirements should be included based on scope, timing, cost and integration considerations

- 3 - Optional** Requirements that pending on scope, timing, cost and integration considerations the State may elect to include in the final Contracted Scope of Work

- 4 – If Available** Requirements that should only be considered should they be available via “Out of the Box” or “configurable” methods using the Offeror proposed solution. Custom development of these items is not permitted under this RFP

Offerors must complete the table as provided and not make any alterations to any rows or columns that have a blue column label which represent the State’s base requirement and priority. The State requires an Offeror response to all green column label cell contents. For those requirements where the State requests that a screen shot be provided or if the Offeror would like to insert a screen shot please insert a “new” row immediately below the requirement that the screen shot is being provided for. Offerors should merge the columns for the inserted row into a single column for the row.

Requirements Matrix Follows

#	Requirement Area	Requirement	Priority	Offeror Proposed Solution	Out of the Box	Configuration Item	Customization Item	Extension/Interface	Other	Offeror Comments
API.1.1	Application Interface	The system must allow the administrative option to secure the user interface against customization by an unauthorized user.	1 - Required							
API.2.2	Application Interface	The system must have a recycle bin to allow users to recover accidentally deleted documents and ensure documents are only permanently deleted from the repository by authorized users, if so configured.	2 - Preferred							
API.3.3	Application Interface	The system must have the ability to create multiple copies of documents, while maintaining a single physical document reference to support document reconciliation needs.	2 - Preferred							
API.4.4	Application Interface	The system must have a flexible and configurable application toolbar for direct access at a minimum: to batches, documents, folders, tasks, reports, workflow, capture, management, and integration settings.	3 - Optional							
API.5.5	Application Interface	The system must have the ability to print and export the rows and columns of text which list documents, batches, folders, and tasks in interactive views.	3 - Optional							
API.6.6	Application Interface	The system must have the ability to take actions on documents, batches, folders, and tasks in interactive views, without being required to open and view the contents of each item.	3 - Optional							
API.7.7	Application Interface	The system must have the ability for use of “drag and drop” to simplify and enhance the moving of objects within, into, and out of document management system windows.	3 - Optional							
API.8.8	Application Interface	The system must provide the user with interactive views based on integration presets, batches, predefined document sets, user-entered searches, folders, tasks, and work flow.	3 - Optional							

#	Requirement Area	Requirement	Priority	Offeror Proposed Solution	Out of the Box	Configuration Item	Customization Item	Extension/Interface	Other	Offeror Comments
API.9.9	Application Interface	The system must have the ability to define a user-specific default view or start-up action in the application's user interface.	4 - If Available							
ARD.1.10	Annotation / Redaction	The system must have the ability for original images in object store remain unaltered by annotations.	2 - Preferred							
ARD.2.11	Annotation / Redaction	The system must have the ability to rapidly change properties of individual annotations and audit a specific annotation's history.	2 - Preferred							
ARD.3.12	Annotation / Redaction	The system must have the ability for user and group-specific annotation security profiles.	3 - Optional							
ARD.4.13	Annotation / Redaction	The system must have the ability for flexible, easy-to-use, secure redaction.	3 - Optional							
ARD.5.14	Annotation / Redaction	The system must have the ability to apply dynamic stamp annotations to images, with options for dynamic date, time, and user name in predefined stamp formats.	3 - Optional							
ARD.6.15	Annotation / Redaction	The system must have the ability to apply predefined stamp annotations to images and create and apply custom stamps.	3 - Optional							
ARD.7.16	Annotation / Redaction	The system must have the ability to print, fax, or export documents with or without all annotations or only visible annotations.	3 - Optional							
ARD.8.17	Annotation / Redaction	The system must have the ability to create customizable text annotations.	3 - Optional							
ARD.9.18	Annotation / Redaction	The system must have the ability to create or append sticky note annotations, with full tracking of text entry by date, time and user.	3 - Optional							
ARD.10.19	Annotation / Redaction	The system must have the ability to support for automatic redaction.	3 - Optional							
ARD.11.20	Annotation / Redaction	The system must have the ability to highlight portions of an image via annotation, with customizable color options.	3 - Optional							
ARD.12.21	Annotation / Redaction	The system must have the ability to support attaching OLE objects and URLs as annotations.	3 - Optional							

#	Requirement Area	Requirement	Priority	Offeror Proposed Solution	Out of the Box	Configuration Item	Customization Item	Extension/Interface	Other	Offeror Comments
ARD.13.22	Annotation / Redaction	The system at a minimum must have the ability to customize and apply multiple variations of line-based annotation tools such as pen, line, arrow, rectangle, and oval.	4 - If Available							
ARD.14.23	Annotation / Redaction	The system must have the ability to create annotations in any color.	4 - If Available							
AUD.1.24	Auditing & Reporting	Based on the exception identified, the system must automatically route exception items from the exception report to a workflow for proper resolution.	2 - Preferred							
AUD.2.25	Auditing & Reporting	The system must allow a system administrator to perform an ad hoc audit on system-related activities from within the client (e.g., identification of all documents accessed by a recently released employee).	3 - Optional							
AUD.3.26	Auditing & Reporting	The system must allow a system administrator to access a document-level audit trail directly from the document.	3 - Optional							
AUD.4.27	Auditing & Reporting	The system must allow a system administrator to create custom audit log entries tied to workflow progress for the purpose of generating business process reports.	3 - Optional							
AUD.5.28	Auditing & Reporting	The system must have a reporting tool which directly integrates with Microsoft Excel, allowing users to build reports natively in Excel utilizing the system attributes.	3 - Optional							
AUD.6.29	Auditing & Reporting	The system must provide reports out-of-the-box that identifies matched, unmatched, or missing numeric and/or character index values between a primary document and secondary document(s) (i.e., automated reconciliation report).	3 - Optional							

#	Requirement Area	Requirement	Priority	Offeror Proposed Solution	Out of the Box	Configuration Item	Customization Item	Extension/Interface	Other	Offeror Comments
AUD.7.30	Auditing & Reporting	The system must provide, within Microsoft Excel, Cognos or other common desktop analysis tools, point-and-click data mining and modeling of text-based reports stored within your repository.	4 - If Available							
CFG.1.31	Configuration	The system allows for ease of configuration, in that most administrative tasks (e.g., adding new document types and index values, user administration, configuring workflows, etc.) can be done by a State government resource versus a third-party systems integrator	2 - Preferred							
CFG.2.32	Configuration	The system must provide a single interface for the configuration and administration of all major system components (e.g., import processing, document type configuration, index value configuration, workflow, user groups and rights, storage structure, scanning, records management, foldering, scripting, etc.).	4 - If Available							
CIM.1-33	Capture and Image Management	The solution must allow for documents to be added in several different ways, including at a minimum the following: <ul style="list-style-type: none"> • Scanning, • Enterprise text report processing, • Electronic forms processing, • Document import processing, • API, • E-mail interface, • Point and click from a business application screen, and • Adding documents already stored within the solution's repository to a workflow process at a specific point-in-time. 	1 - Required							
CIM.2.34	Capture and Image Management	The System will include the separation of image and PDF file types.	1 - Required							

#	Requirement Area	Requirement	Priority	Offeror Proposed Solution	Out of the Box	Configuration Item	Customization Item	Extension/Interface	Other	Offeror Comments
CIM.3.35	Capture and Image Management	The system must have the ability to migrate documents and metadata from third party applications such as ePAR and ePerformance from the OAKS HCM System.	1 - Required							
CIM.4.36	Capture and Image Management	The system must have the ability to upload scanned batches directly to the server.	1 - Required							
CIM.5.37	Capture and Image Management	For instance, at a minimum the solution should provide options for QA image quality and/or index accuracy.	1 - Required							
CIM.6.38	Capture and Image Management	It should also provide a simple image re-scan process that automatically replaces the poor images with the newly-scanned images.	1 - Required							
CIM.7.39	Capture and Image Management	The system must have the ability to integrate with other devices (fax, Multi-function copier scanner devices) as a means of ingesting documents into the system.	2 - Preferred							
CIM.8.40	Capture and Image Management	The system must have the ability to capture a batch process that allows for page separation and retrieval.	2 - Preferred							
CIM.9.41	Capture and Image Management	The system must have the ability for batch scanning capabilities for high-volume production environment.	2 - Preferred							
CIM.10.42	Capture and Image Management	The system at a minimum must have the ability to configure, save, and apply scanner settings such as resolution, page size, orientation, brightness, threshold, and image processing.	2 - Preferred							
CIM.11.43	Capture and Image Management	The system must have the ability to control and track the modification of documents through multiple revisions, allowing users to view prior revisions and track document history. The solution should clearly display the number of revisions associated with a specific document. The solution should allow for the addition of comments per revision.	2 - Preferred							

#	Requirement Area	Requirement	Priority	Offeror Proposed Solution	Out of the Box	Configuration Item	Customization Item	Extension/Interface	Other	Offeror Comments
CIM.12.44	Capture and Image Management	The system at a minimum must have the ability to configure, name, save, select, and distribute capture settings such as document source, proposed index keys, workflow routing, and OCR and page content indexing.	2 - Preferred							
CIM.13.45	Capture and Image Management	When a completed ePAR with supporting document has already been imported, the system can import a new supporting document associated to the relevant ePAR.	2 - Preferred							
CIM.14.46	Capture and Image Management	The system must have the ability to support both centralized and decentralized scanning operations, including remote scanning from/to multiple locations	2 - Preferred							
CIM.15.47	Capture and Image Management	The system should be capable of rotating images to right side up.	2 - Preferred							
CIM.16.48	Capture and Image Management	The system must be compatible with Kofax Virtual Rescan (VRS) scanning software.	2 - Preferred							
CIM.17.49	Capture and Image Management	The system must be compatible with TWAIN compatible scanning software.	2 - Preferred							
CIM.18.50	Capture and Image Management	The system must have the ability to automatically classify and index images.	3 - Optional							
CIM.19.51	Capture and Image Management	The system must have the ability to save scanned images in open, industry-standard graphics format.	3 - Optional							
CIM.20.52	Capture and Image Management	The system must have the ability to automatically fill several index values on a document based on a primary index value that triggers the automatic look up of additional index information already contained within the system.	3 - Optional							

#	Requirement Area	Requirement	Priority	Offeror Proposed Solution	Out of the Box	Configuration Item	Customization Item	Extension/Interface	Other	Offeror Comments
CIM.21.53	Capture and Image Management	The system must have the ability provide data and text extraction capabilities for scanned image documents, including at a minimum: OCR, ICR, OMR, bar codes, and signature detection, in order to provide hands-off processing of scanned documents directly into the system without involving third party software applications.	3 - Optional							
CIM.22.54	Capture and Image Management	The system must have the ability to associate an electronic signature with a managed workflow event.	3 - Optional							
CIM.23.55	Capture and Image Management	The system must have the ability to support a full range of entry-level to high-speed scanners from a choice of manufacturers, with options including at a minimum: simplex and duplex, monochrome, color, paper size, paper weight, etc.	3 - Optional							
CIM.24.56	Capture and Image Management	The system must have the ability to support deletion of blank pages during scanning.	3 - Optional							
CIM.25.57	Capture and Image Management	The system at a must have the ability to perform quality assurance (QA) / verification of captured image documents. For instance, at a minimum the solution should provide options for QA image quality and/or index accuracy. It should rotate images to right side up. It should also provide a simple image re-scan process that automatically replaces the poor images with the newly-scanned images.	3 - Optional							
CIM.26.58	Capture and Image Management	The system must have the ability to stamp a specific revision of a document as a version, limiting which revisions of a document a certain user can see.	3 - Optional							
CIM.27.59	Capture and Image Management	The system must have the ability to send a predefined captured document type to a targeted repository.	3 - Optional							

#	Requirement Area	Requirement	Priority	Offeror Proposed Solution	Out of the Box	Configuration Item	Customization Item	Extension/Interface	Other	Offeror Comments
CIM.28.60	Capture and Image Management	The system must have the ability to perform quality assurance (QA) on images when capturing or can bypass QA if desired.	3 - Optional							
CIM.29.61	Capture and Image Management	The system must have the ability to scan batches locally and upload batches to server at a time the user specifies.	3 - Optional							
CIM.30.62	Capture and Image Management	The system must have the ability to capture and index documents for remote users and devices	3 - Optional							
CIM.31.63	Capture and Image Management	The system must have the ability to send scanned output directly to the Offeror's proposed workflow engine.	3 - Optional							
CIM.32.64	Capture and Image Management	The system must have the ability for one central GUI for administration and deployment of capture products.	3 - Optional							
CIM.33.65	Capture and Image Management	The system must support scanning within a Virtual Desktop (e.g., Citrix, Wyse, etc.) environment.	4 - If Available							
CIM.34.66	Capture and Image Management	The system must have the ability to distribute and load balance an even portion of quality assured scanned batches to assigned locations/users outside of the scanning location.	4 - If Available							
CIM.35.67	Capture and Image Management	The system at a minimum must be able to ingest advanced print streams such as AFP, DJDE, PCL, or PDF.	4 - If Available							
CIM.36.68	Capture and Image Management	The system must have the ability for scanning through the Microsoft SharePoint interface.	4 - If Available							
CIM.37.69	Capture and Image Management	The system must have the ability to easily and quickly configure the ingestion of print streams.	4 - If Available							
DCT.1.70	Document Control	The system must have document control flexibility, allowing individual use or group collaboration.	1 - Required							
DCT.2.71	Document Control	The system must have the ability to track document control activities.	1 - Required							

#	Requirement Area	Requirement	Priority	Offeror Proposed Solution	Out of the Box	Configuration Item	Customization Item	Extension/Interface	Other	Offeror Comments
DCT.3.72	Document Control	The system must support public-key infrastructure (PKI) is a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates. Suite B is a set of cryptographic algorithms specified by the National Security Agency (NSA) as part of an effort to modernize information assurance capabilities. Suite B algorithms are intended to be used to secure unclassified information and most classified information.	1 - Required							
DCT.4.73	Document Control	The system must provide different metadata types (i.e. date, date and time, currency, specific currency, alphanumeric, numeric, floating point) and import export common file formats including at a minimum: .bak - System Backup Files, .dat - data files, .doc, .docx, .dot - Microsoft Word, .gif, .tiff, .jpg, .bmp - Graphics, .html - Hypertext Markup Language, .mdb - Microsoft Access Database Files, .mpp - Microsoft Project, .pdf - Adobe Acrobat, .ppt, .pptx - MS PowerPoint, .rtf - Rich Text Format, .txt - ASCII Text, .vsd - Microsoft Visio, .wpd, .wp5 - WordPerfect, .xls, .xlsx, .wks - Microsoft Excel, and .xml - Extensible Markup Language.	1 - Required							
DCT.5.74	Document Control	the system must export both content and properties.	1 - Required							
DCT.6.75	Document Control	The system should support Document sharing or collaboration via roles and security for documents that belong to two or more offices or workgroups	1 - Required							

#	Requirement Area	Requirement	Priority	Offeror Proposed Solution	Out of the Box	Configuration Item	Customization Item	Extension/Interface	Other	Offeror Comments
DCT.7.76	Document Control	The system must have document control to incorporate digital signatures based on stringent Suite B and PKI standards.	2 - Preferred							
DCT.8.77	Document Control	The system must have the ability for industry-standard document library services.	2 - Preferred							
DCT.9.78	Document Control	The system must have document control options for multiple client types and extends document control and digital signatures directly to interfaces of third-party applications.	4 - If Available							
DCT.10.79	Document Control	The system must have the ability to edit text directly within the document viewer.	4 - If Available							
DPR.1.80	Document Properties	The system will allow only authorized users to output document content or renditions.	2 - Preferred							
DPR.2.81	Document Properties	The system supports an unlimited number of document types within the system.	2 - Preferred							
DPR.3.82	Document Properties	The system must support the following types of Document Output at a minimum: • Viewing, • Printing, and • Exporting.	2 - Preferred							
DPR.4.83	Document Properties	The system must provide the ability to pre-populate an addendum from RTF template.	3 - Optional							
DPR.5.84	Document Properties	The system must have the ability to create documents as encrypted PDF.	3 - Optional							
DPR.6.85	Document Properties	The system must provide the ability to define multiple instances of the same property value field to a single document.	3 - Optional							
DPR.7.86	Document Properties	The system must allow values for properties to be selected from lists maintained both inside and outside of the system.	3 - Optional							
DPR.8.87	Document Properties	The system must be able to validate or select property values from its own data dictionary or from data tables of other external applications.	3 - Optional							

#	Requirement Area	Requirement	Priority	Offeror Proposed Solution	Out of the Box	Configuration Item	Customization Item	Extension/Interface	Other	Offeror Comments
DPR.9.88	Document Properties	The system must be able to accommodate spell checking of all text attributes fields.	4 - If Available							
DHR.1.89	Document Hierarchy Requirements	The system must allow the end user to specify the properties required to properly identify and store the document.	3 - Optional							
DHR.2.90	Document Hierarchy Requirements	The system must allow rules to govern the storage hierarchies to be defined for each document type and sub-type combination.	3 - Optional							
DHR.3.91	Document Hierarchy Requirements	The system must automatically create the storage hierarchies and link the document into proper storage structure.	3 - Optional							
DHR.4.92	Document Hierarchy Requirements	The system must allow property values, literal text, or a combination of both as the label for a folder.	3 - Optional							
DHR.5.93	Document Hierarchy Requirements	If the document classification changes (due to property changes) the system must automatically update the storage hierarchy to match the classification changes.	3 - Optional							
DHR.6.94	Document Hierarchy Requirements	The system must automatically link documents into the proper hierarchies based on specific property values.	3 - Optional							
DHR.7.95	Document Hierarchy Requirements	If the storage hierarchies do not exist, the system must automatically create them prior to linking in the document from its physical data storage location.	3 - Optional							
DHR.8.96	Document Properties	The system will ensure that display only Properties will be clearly distinguishable as such by users.	4 - If Available							
DHR.9.97	Document Hierarchy Requirements	The system must have the ability to link the physical data storage location of a document to multiple storage hierarchies.	4 - If Available							
DVR.1.98	Document Viewer	The system must have the ability to rotate documents in document viewer and save rotated views.	2 - Preferred							

#	Requirement Area	Requirement	Priority	Offeror Proposed Solution	Out of the Box	Configuration Item	Customization Item	Extension/Interface	Other	Offeror Comments
DVR.2.99	Document Viewer	The system must have the ability for the document viewer to display a wide range of digital object types in their native formats, including at a minimum: Microsoft Office, PDF, JPEG, TIFF, HTML, XML, and audio/video media files; with functional permission granted by user role.	2 - Preferred							
DVR.3.100	Document Viewer	The system must have the ability to perform common operations such as re-index, copy, email, export, print, fax, and delete pages within document view interface; with functional permission granted by user role.	2 - Preferred							
DVR.4.101	Document Viewer	The system must have the ability to cross referenced documents between the currently displayed documents to a display of related documents.	2 - Preferred							
DVR.5.102	Document Viewer	The system must have the ability to reorder pages within the document view interface, and add pages to existing document; with functional permission granted by user role.	2 - Preferred							
DVR.6.103	Document Viewer	The system must have the ability to copy or move pages from one document to another from within the document view interface; with functional permission granted by user role.	2 - Preferred							
DVR.7.104	Document Viewer	The system must have the ability to display documents side-by-side with records in the business application.	3 - Optional							
DVR.8.105	Document Viewer	The system must have the ability for the single-page viewing.	3 - Optional							
DVR.9.106	Document Viewer	The system must have the ability for incremental zooming in options in the document viewer	3 - Optional							
DVR.10.107	Document Viewer	The system must have the ability to copy and paste document text.	3 - Optional							

#	Requirement Area	Requirement	Priority	Offeror Proposed Solution	Out of the Box	Configuration Item	Customization Item	Extension/Interface	Other	Offeror Comments
DVR.11.108	Document Viewer	The system must have the ability to apply document annotations such as stamps, sticky notes, text, and redactions to bitmap images directly within document view interface; with functional permission granted by user role.	3 - Optional							
DVR.12.109	Document Viewer	The system must have the ability to open a viewer-displayed document in an associated application (e.g., MS Word, MS Excel, etc.) for viewing or editing.	3 - Optional							
DVR.13.110	Document Viewer	The system must have the ability for the document viewer to be flexible, user-configurable display of index keys, document properties, document notes, predefined actions, tasks, page thumbnails, associated eForms, and toolbars.	3 - Optional							
DVR.14.111	Document Viewer	The system must have the ability for integrated view enhancement options such as on-screen image inversion (reverse black and white) and smoothing; with functional permission granted by user role.	3 - Optional							
DVR.15.112	Document Viewer	The system must have a convenient and flexible page selection interface within document viewer.	3 - Optional							
DVR.16.113	Document Viewer	The system must have the ability for multiple view panning options to easily adjust current position of viewed area on magnified image.	3 - Optional							
DVR.17.114	Document Viewer	The system must have the ability to designate documents for collection into user-defined project groupings directly from document viewer, without using index values.	3 - Optional							
DVR.18.115	Document Viewer	The system must have the ability to add documents to a workflow or route documents within a workflow directly from the document viewer.	3 - Optional							

#	Requirement Area	Requirement	Priority	Offeror Proposed Solution	Out of the Box	Configuration Item	Customization Item	Extension/Interface	Other	Offeror Comments
DVR.19.116	Document Viewer	The system must have the ability for an integrated display of a document's search-targeted content when opening a full-document image found via content search text indexed.	3 - Optional							
DVR.20.117	Document Viewer	The system must have the ability for the document viewer to work with familiar, existing desktop email platforms (MS Outlook is the State's standard) to simplified sending images (or links to images) to email recipients outside of the imaging system's workflow.	4 - If Available							
DVR.21.118	Document Viewer	The system must have the ability for emailed documents or document links directly from document viewer interface, with options for page selection, annotation inclusion, multi-page TIFF generation, selectable headers and footers, and file renaming.	4 - If Available							
DVR.22.119	Document Viewer	The system at a minimum must have the ability for the multi-page (MDI), PDF and TIFF viewing - display two or more pages simultaneously on the user's screen.	4 - If Available							
EML.1.120	E-Mail	The system must have the ability for a user to access the system's workflow processes from the e-mail client interface, with the ability to decision items (execute tasks) and view related documents directly from the e-mail message notification. Note: The State's desktop productivity tools (standard) is Microsoft Office, including Microsoft Outlook	3 - Optional							
EML.2.121	E-Mail	The system must allow a point and click method to import messages into the system using e-mail client folders in order to automate the classification and indexing of e-mails and attachments (e.g., a user could create a folder for ePARS, ePerformance, Benefits, Discipline, etc.)	3 - Optional							

#	Requirement Area	Requirement	Priority	Offeror Proposed Solution	Out of the Box	Configuration Item	Customization Item	Extension/Interface	Other	Offeror Comments
EML.3.122	E-Mail	The system provides the ability to search on e-mail index values and/or perform a full-text search on e-mail and attachment content.	4 - If Available							
IDX.1.123	Indexing / Advanced Metadata	The system must support the organization of documents into folder-type structures.	1 - Required							
IDX.2.124	Indexing / Advanced Metadata	The system at a minimum must have the ability to index documents with user-configurable data elements not taken from the host such as date/time, unique ID, serial number, predefined list, and free-form text entry application.	2 - Preferred							
IDX.3.125	Indexing / Advanced Metadata	The system must have the ability to index multiple documents as a group without re-entering index values for each page.	2 - Preferred							
IDX.4.126	Indexing / Advanced Metadata	The system must have the ability to easily pre-define document relationships for use in search and retrieval.	2 - Preferred							
IDX.5.127	Indexing / Advanced Metadata	The system must have the ability to re-index documents via manual entry or single click associated with host records.	2 - Preferred							
IDX.6.128	Indexing / Advanced Metadata	The system must provide a means of purging with appropriate permissions, with just a few clicks, those index values that are no longer being used (saving database space and optimizing performance).	2 - Preferred							
IDX.7.129	Indexing / Advanced Metadata	The system must offer the ability to create and assign custom indexing based on document type.	2 - Preferred							
IDX.8.130	Indexing / Advanced Metadata	The system must support an unlimited number of index values per document.	2 - Preferred							
IDX.9.131	Indexing / Advanced Metadata	The system must have the ability to configure and select pre-defined index values via a drop-down menu or "pick list."	3 - Optional							

#	Requirement Area	Requirement	Priority	Offeror Proposed Solution	Out of the Box	Configuration Item	Customization Item	Extension/Interface	Other	Offeror Comments
IDX.10.132	Indexing / Advanced Metadata	The system must provide a dedicated "Document Type" index value class for documents and control security. Used "index value" vs. index key in revised text.	3 - Optional							
IDX.11.133	Indexing / Advanced Metadata	The system must provide a point-and-click configuration for index values, with multiple pre-configured formats (e.g., date: dd/mm/yyyy, month/dd/yy, mm-dd-yy).	3 - Optional							
IDX.12.134	Indexing / Advanced Metadata	The system must provide the ability to store index value sets that can later be used to auto-index documents by entry of only a single primary value. This enables simplified indexing and more flexible retrieval by allowing users to enter a single index value and have all related index values auto-populate.	3 - Optional							
IDX.13.135	Indexing / Advanced Metadata	The system must have the ability to automatically index documents, based on a single known document type, through the retrieval and application of related index values from an external database.	3 - Optional							
IDX.14.136	Indexing / Advanced Metadata	The system must have the ability for individual documents to be easily to be indexed "same as last document".	3 - Optional							
IDX.15.137	Indexing / Advanced Metadata	The system must provide indexing options that are flexible and customizable.	3 - Optional							
IDX.16.138	Indexing / Advanced Metadata	The system must provide indexing options among workstations and locations.	3 - Optional							
IDX.17.139	Indexing / Advanced Metadata	The system must have the ability to index from OCR scans.	3 - Optional							
IDX.18.140	Indexing / Advanced Metadata	The system must have the ability to automatically and periodically validate existing document types against an external database.	3 - Optional							
IDX.19.141	Indexing / Advanced Metadata	The system must provide user indexing options prior to scanning.	3 - Optional							

#	Requirement Area	Requirement	Priority	Offeror Proposed Solution	Out of the Box	Configuration Item	Customization Item	Extension/Interface	Other	Offeror Comments
IDX.20.142	Indexing / Advanced Metadata	The system must read bar codes during capturing to index documents.	3 - Optional							
IDX.21.143	Indexing / Advanced Metadata	The system must have the ability to use single keystrokes to index multiple fields during batch processing.	3 - Optional							
INT.1.144	Integration	The system must provide a detailed description of API and Web Service feature set, use and usage.	2 - Preferred							
INT.2.145	Integration	The system must have the ability to integration via web services standards.	2 - Preferred							
INT.3.146	Integration	The system must have options for both programmatic and non-programmatic integration.	2 - Preferred							
INT.4.147	Integration	The system must provide http URL requests to retrieve documents, present workflow interfaces, and present a folder interface in lieu of custom programming.	3 - Optional							
INT.5.148	Integration	The system must have extended integration functionality that allows placement of imaging application icon in the screens of business applications to initiate document retrieval or other actions in the imaging system.	3 - Optional							
INT.6.149	Integration	The proposed DMS solution must provide integration support with email (Microsoft Outlook), allowing users to access functionality and import emails and attached documents into the repository directly from their email interface.	4 - If Available							
INT.7.150	Integration	The system must direct integration with many business applications without programming.	4 - If Available							
INT.8.151	Integration	The system must have a graphical user interface allowing visual, interactive, centralized design and testing of application integration configurations non-programmatic.	4 - If Available							

#	Requirement Area	Requirement	Priority	Offeror Proposed Solution	Out of the Box	Configuration Item	Customization Item	Extension/Interface	Other	Offeror Comments
INT.9.152	Integration	The system must have non-programmatic configuration that will enable the system to be auto-aware of any business application that is integrated for document retrievals (meaning a user does not have to manually declare the business system in which they are working).	4 - If Available							
INT.10.153	Integration	The system must have non-programmatic integration with Windows applications.	4 - If Available							
INT.11.154	Integration	The system must have non-programmatic integration with browser-delivered applications.	4 - If Available							
PFO.1.155	Printing / Faxing / Output	The system must have the option to selectively export files in alternate formats including at a minimum: PDF, TIFF.	1 - Required							
PFO.2.156	Printing / Faxing / Output	The system must have the ability to print to any print device within a platform's standard desktop/network printing environment.	2 - Preferred							
PFO.3.157	Printing / Faxing / Output	The system must have the ability to print documents with or without all annotations or only visible annotations.	2 - Preferred							
PFO.4.158	Printing / Faxing / Output	The system must have the ability to print multiple pages from a selected range.	2 - Preferred							
PFO.5.159	Printing / Faxing / Output	The system must have the ability to control printing permissions through application security; (i.e. restrictions on document type).	2 - Preferred							
PFO.6.160	Printing / Faxing / Output	The system must have the ability to print single selected pages within a multi-page document.	2 - Preferred							
PFO.7.161	Printing / Faxing / Output	The system must offer the option to export files in their native format or another preselected format such as PDF or TIFF.	3 - Optional							
PFO.8.162	Printing / Faxing / Output	The system must have the ability to print documents from a list view such as search results or workflow queue, without opening each document.	3 - Optional							

#	Requirement Area	Requirement	Priority	Offeror Proposed Solution	Out of the Box	Configuration Item	Customization Item	Extension/Interface	Other	Offeror Comments
PFO.9.163	Printing / Faxing / Output	The system must have the ability to print a document list, rather than the documents themselves, from a list view such as search results or a workflow queue.	3 - Optional							
PFO.10.164	Printing / Faxing / Output	The system must meet Department of Labor document retention and reporting requirements for I9s for employees (active and inactive) – a summary report (inventory) as well as all I9s on File (detail)	1 - Required							
PFO.11.165	Printing / Faxing / Output	The system must have the ability to print for integrated outbound faxing.	3 - Optional							
PFO.12.166	Printing / Faxing / Output	The system must have the ability to automate the printing and exporting triggered by workflow events, server APIs, other application modules, or values generated by external applications.	4 - If Available							
PFO.13.167	Printing / Faxing / Output	The system must have the ability to save, recall, and secure predefined output configurations for the control of automated document output, including options for native and converted file export, emailing, printing, and faxing.	4 - If Available							
PFO.14.168	Printing / Faxing / Output	The system must have the ability to selectively overprint relevant document values such as page number, date and time, and document keys on each page.	4 - If Available							
RMG.1.169	Records Management	The system must not purge related entries from the audit trail during a document purge.	1 - Required							
RMG.2.170	Records Management	The system must have the ability to require approvals on disposition of a document.	1 - Required							
RMG.3.171	Records Management	The system must create reports with retention data. Offerors should provide a list of their proposed DMS solution's standard reports.	1 - Required							

#	Requirement Area	Requirement	Priority	Offeror Proposed Solution	Out of the Box	Configuration Item	Customization Item	Extension/Interface	Other	Offeror Comments
RMG.4.172	Records Management	The system must at a minimum allow users to capture, declare, and store electronic records (documents) in their native formats, including e-mail, electronic forms, physical items, images, text files, and Microsoft Office documents.	2 - Preferred							
RMG.5.173	Records Management	The system must have the ability to place a hold (or multiple holds) on a record, as in the case of an audit or legal discovery.	2 - Preferred							
RMG.6.174	Records Management	The system must provide the ability to assign retention schedules to documents or groups of documents based on a variety of dates.	2 - Preferred							
RMG.7.175	Records Management	The system must provide alerts and messaging when documents reach end of cycle on their given retention schedule.	2 - Preferred							
RMG.8.176	Records Management	System must allow for multiple documents to be grouped together and treated by the system as one document type linked to a retention rule.	2 - Preferred							
RMG.9.177	Records Management	The system must physically (permanently) delete a document(s) based on the retention schedule.	2 - Preferred							
RMG.10.178	Records Management	The system must provide easily defined, rules-based retention and disposition policies.	3 - Optional							
RMG.11.179	Records Management	The system must when completing a document purging process create an entry in the audit trail.	3 - Optional							
RMG.12.180	Records Management	The system must provide support for automated document dispositions and transfers.	3 - Optional							
RMG.13.181	Records Management	The system must provide records management ability that does not require an additional module or third party tool.	3 - Optional							
RMG.14.182	Records Management	The system must create litigation and audit holds which prevent modification and deletion of information.	3 - Optional							

#	Requirement Area	Requirement	Priority	Offeror Proposed Solution	Out of the Box	Configuration Item	Customization Item	Extension/Interface	Other	Offeror Comments
RMG.15.183	Records Management	The system must be able to send a notification to defined users prior to purging documents.	3 - Optional							
RMG.16.184	Records Management	The system must provide the ability for a document(s) to be dragged and dropped into a record (folder of documents) and have this new document automatically inherit the records management policy. (i.e. Retention Rules)	3 - Optional							
RMG.17.185	Records Management	The system must have the ability to link retention rules to document types that will automatically engage the retention rule.	3 - Optional							
RMG.18.186	Records Management	The system must have the ability to track information lifecycle with comprehensive auditing.	3 - Optional							
RMG.19.187	Records Management	The system must have the ability to identify both complete and incomplete records across the entire repository.	3 - Optional							
RMG.20.188	Records Management	The system must be configurable to automatically purge "Draft" versions (and associated PDF Renditions and annotations) of a document after a specified number of days have elapsed following a document's promotion to "Approved."	3 - Optional							
RMG.21.189	Records Management	The system must have the ability for documents to be automatically declared as records without any user interaction.	3 - Optional							
RMG.22.190	Records Management	The system at a minimum must provide an administrative view of physical record locators either pending check out (requested) or currently checked out with appropriate location information (item name, user in possession, expected return date, identifier, repository, repository name).	3 - Optional							

#	Requirement Area	Requirement	Priority	Offeror Proposed Solution	Out of the Box	Configuration Item	Customization Item	Extension/Interface	Other	Offeror Comments
RMG.23.191	Records Management	The system must provide a variety of destruction options, including at a minimum: the ability to keep both index values and files permanently, keep only index values, or purge both index values and files with or without a history log (certificate of destruction).	3 - Optional							
RMG.24.192	Records Management	The system must manage retention policies to track the physical location of paper documents	4 - If Available							
RMG.25.193	Records Management	The system must provide a holistic view of both digitally-stored content and physically stored content in a single search results list.	4 - If Available							
RPT.1.194	Reporting/Business Intelligence	The system must have comprehensive set of business intelligence features to provide workflow, security, content and data deficiencies, and user activity reporting through the familiar DMS interface.	3 - Optional							
RPT.2.195	Reporting/Business Intelligence	The system must have the ability to present reports and dashboards to all users or restrict reporting to authorized users.	3 - Optional							
RPT.3.196	Reporting/Business Intelligence	The system must have the ability to schedule, execute, view, and distribute report instances at a minimum to all users, specific users.	3 - Optional							
RPT.4.197	Reporting/Business Intelligence	The system must have dashboard capabilities to provide users with an at-a-glance overview of system supported business processes.	4 - If Available							
RPT.5.198	Reporting/Business Intelligence	The system must have an intuitive selection for business users to create and modify reports and dashboards.	4 - If Available							
RPT.6.199	Reporting/Business Intelligence	The system must have a comprehensive report library with ongoing report definition development based on user input.	4 - If Available							
RPT.7.200	Enterprise Report Management	The system must have the ability to provide an enterprise report user interface optimized for searching, viewing, and previewing report documents.	4 - If Available							

#	Requirement Area	Requirement	Priority	Offeror Proposed Solution	Out of the Box	Configuration Item	Customization Item	Extension/Interface	Other	Offeror Comments
RPT.8.201	Enterprise Report Management	The system must have the ability to allow searches against line item values, not just index values.	4 - If Available							
RPT.9.202	Enterprise Report Management	The system must provide user access to select, formatted pages related to records in the business application, such as a single image/page from a large print stream.	4 - If Available							
RPT.10.203	Enterprise Report Management	The system must have the ability to define a different set of graphical form overlays for each type of print stream.	4 - If Available							
RPT.11.204	Enterprise Report Management	The system must have the ability to capture a wide variety of print output from line-of-business systems and convert into searchable, non-proprietary PDF files	4 - If Available							
RPT.12.205	Enterprise Report Management	The system must have the ability to capture basic and advanced print streams e.g., ASCII, EBCDIC text, PDF, IBM AFP, Xerox, Metacode, HP PCL, and PostScript formats.	4 - If Available							
RPT.13.206	Enterprise Report Management	The system must have the ability to monitor a different directory for each type of print stream.	4 - If Available							
RSP.1.207	Retrieval / Search / Presentation	The system must have the ability to search documents, and folders, via a single search condition relevant to the context currently being viewed.	2 - Preferred							
RSP.2.208	Retrieval / Search / Presentation	The system must provide integrated document retrieval from business applications; single-click access to documents from any record displayed.	2 - Preferred							
RSP.3.209	Retrieval / Search / Presentation	The system must provide the ability to execute separate and distinct document retrievals from sections/fields on the screen.	3 - Optional							
RSP.4.210	Retrieval / Search / Presentation	The system must have the ability to search on and find text located within the results grid.	3 - Optional							
RSP.5.211	Retrieval / Search / Presentation	The system must have the ability to secure saved searches and the presentation of documents and folders by both individual user and group.	3 - Optional							

#	Requirement Area	Requirement	Priority	Offeror Proposed Solution	Out of the Box	Configuration Item	Customization Item	Extension/Interface	Other	Offeror Comments
RSP.6.212	Retrieval / Search / Presentation	The system must have the ability to conduct a full-text search of the scanned document for a wide range of native document formats simultaneously, with both full text and natural language defined and variable conditions such as current user name or current record value in an external application.	3 - Optional							
RSP.7.213	Retrieval / Search / Presentation	The system must have the ability to display item sort order, before or after a search, using any combination of item metadata individually designated as ascending or descending.	3 - Optional							
RSP.8.214	Retrieval / Search / Presentation	From a data-centric business application, based on account/record information presented on the screen, system must allow users to retrieve stored documents without custom programming, API programming, scripting, or modifications to the existing application.	3 - Optional							
RSP.9.215	Retrieval / Search / Presentation	The system must have the ability for both individual users and groups to customize and save the presentation of search queries by column configuration, sort order, and grouping of documents.	3 - Optional							
RSP.10.216	Retrieval / Search / Presentation	The system must have the ability to build and execute searches for enterprise reports from the same familiar interface as that used for simple, complex, and full text searches.	4 - If Available							
RSP.11.217	Retrieval / Search / Presentation	The system must have the ability to group the display of documents and folders in any list view.	4 - If Available							
RSP.12.218	Retrieval / Search / Presentation	The system must have the ability to display calculated statistics about the documents and document properties contained within a list view.	4 - If Available							

#	Requirement Area	Requirement	Priority	Offeror Proposed Solution	Out of the Box	Configuration Item	Customization Item	Extension/Interface	Other	Offeror Comments
RSP.13.219	Retrieval / Search / Presentation	The system must have the ability for both individual users and groups to store, customize and refine the standard conditions of saved searches.	4 - If Available							
SEC.1.220	Security	The system must provide audit options when logging client, server, and user authentication actions.	1 - Required							
SEC.2.221	Security	The system must allow audit actions of defined clients from an administrative interface.	1 - Required							
SEC.3.222	Security	The system must have server storage subsystem with encrypted object path metadata, secure object store connectivity (no client-level direct access or drive mapping required) and the availability of volume-level data protection.	2 - Preferred							
SEC.4.223	Security	The system must have document access control via logical filing hierarchy.	2 - Preferred							
SEC.5.224	Security	The system at a minimum must allow multiple user authentication options which build on the State of Ohio's existing security infrastructure, including user names, passwords, and identity servers (Identify whether your response applies to a customer-hosted or a vendor-hosted solution.)	2 - Preferred							
SEC.6.225	Security	The system must provide for the management and administration control of access to folder types.	2 - Preferred							
SEC.7.226	Security	The system must have control access to integration presets; with functional permission granted by user role.	2 - Preferred							
SEC.8.227	Security	The system must have the ability to control and manage all workflow processes or only specific ones.	2 - Preferred							
SEC.9.228	Security Administration	The system must support the ability to define and assign permission sets for each document type and sub-type.	2 - Preferred							

#	Requirement Area	Requirement	Priority	Offeror Proposed Solution	Out of the Box	Configuration Item	Customization Item	Extension/Interface	Other	Offeror Comments
SEC.10.229	Security Administration	The system must automatically apply the proper permission set to a document upon lifecycle and state change.	2 - Preferred							
SEC.11.230	Security Administration	The proposed DMS system must at minimum provide the following system permission levels based on roles: <ul style="list-style-type: none"> • No Access • Read Only • Annotate/Update • Write • Version • Delete • Print • Email • Report • Properties • Re-index 	2 - Preferred							
SEC.12.231	Security	The system must have encrypted communication between server and clients.	3 - Optional							
SEC.13.232	Security	The system must have the ability to copy user and group privileges to simplify security configuration.	3 - Optional							
SEC.14.233	Security	The system must control users' actions on documents based on defined "document type" value.	3 - Optional							
SEC.15.234	Security	The system must control users' batch access.	3 - Optional							
SEC.16.235	Security	The system must have control document access via workflow queue.	3 - Optional							
SEC.17.236	Security	The system must have an automatic client log-off which can be initiated by a new log-on from a different location.	3 - Optional							
SSA.1.237	Server/System Administration	The system must have the ability to audit all actions of all clients as viewed from the administrative interface.	1 - Required							
SSA.2.238	Server/System Administration	The system must enable authorized users to manage users, groups, and permissions.	1 - Required							
SSA.3.239	Server/System Administration	The system must have the ability to add new users in bulk from the Windows domain, LDAP server, text file, or local machine.	1 - Required							

#	Requirement Area	Requirement	Priority	Offeror Proposed Solution	Out of the Box	Configuration Item	Customization Item	Extension/Interface	Other	Offeror Comments
SSA.4.240	Server/System Administration	The system must make available automatic synchronization of the DMS system users and groups with those on an LDAP server, LDAP-enabled Active Directory server, or ID Domain.	1 - Required							
SSA.5.241	Server/System Administration	The system must be able to operate in a virtualized environment based on VMware.	1 - Required							
SSA.6.242	Server/System Administration	The system must have the ability to disable user accounts without deleting them.	2 - Preferred							
SSA.7.243	Server/System Administration	The system must follow DAS/OIT requirements for disaster recovery and business continuity.	2 - Preferred							
SSA.8.244	Server/System Administration	The system must support LDAP, Active Directory, and ID Domain authentication.	2 - Preferred							
SSA.9.245	Server/System Administration	The system must have API capabilities for external applications to retrieve and insert documents.	2 - Preferred							
SSA.10.246	Server/System Administration	The system must enable authorized users to manage supported file formats and system configurations.	2 - Preferred							
SSA.11.247	Server/System Administration	The system must allow for the segregation (and delegation) of system administration functions to authorized users.	2 - Preferred							
SSA.12.248	Server/System Administration	The system must be available 98.5% during normal business hours of Monday-Friday to users, and additional system maintenance functions including backup and batch operations should be performed outside of these hours	3 - Optional							
SSA.13.249	Server/System Administration	If acquired on a named user license arrangement, licenses must be transferable within the organization.	3 - Optional							
SSA.14.250	Server/System Administration	The system must have the ability to monitor user software license availability and usage from administrative interface.	3 - Optional							

#	Requirement Area	Requirement	Priority	Offeror Proposed Solution	Out of the Box	Configuration Item	Customization Item	Extension/Interface	Other	Offeror Comments
SSA.15.251	Server/System Administration	The system must at a minimum allow an administrator to view real-time list of logged-on clients, with information about server instance, server host, IP address, and time connected.	3 - Optional							
SSA.16.252	Server/System Administration	The system must display the screen to perform a function within 3 seconds after the function is selected by a user.	3 - Optional							
SSA.17.253	Server/System Administration	The system must have the ability to automatically distribute and capture device profiles to clients.	3 - Optional							
SSA.18.254	Server/System Administration	The system must enable authorized users to manage repository data dictionaries.	3 - Optional							
SSA.19.255	Server/System Administration	The system must have the ability to send messages to individual imaging system users or all users currently logged on directly from the server.	4 - If Available							
SSA.20.256	Server/System Administration	The proposed DMS system must allow for the import of user information from a text file, which includes multiple delimiter types and interactive field mapping.	4 - If Available							
SSA.21.257	Server/System Administration	The system must have a graphical administrator interface accessible from the client.	4 - If Available							
SSA.22.258	Server/System Administration	The system must have integrated server-side tools to provide on-demand performance analysis of server processes.	4 - If Available							
SSA.23.259	Server/System Administration	The system must support the use of Citrix and other virtual clients.	4 - If Available							
SSA.24.260	Server/System Administration	The system must provide multiple security options for logging into the system, which should allow the system administrator to decide which option is the best (e.g., using a separate security model for an additional logon and password, NT Authentication, integration with Windows Active Directory or LDAP single sign-on authentication).	2 - Preferred							

#	Requirement Area	Requirement	Priority	Offeror Proposed Solution	Out of the Box	Configuration Item	Customization Item	Extension/Interface	Other	Offeror Comments
STG.1.261	Storage	The system must store source documents in their original, native file formats, not in a proprietary format that can be accessed independent of the system.	1 - Required							
STG.2.262	Storage	System's storage architecture allows for documents and images to be stored one too many different physical locations for the purpose of redundancy. If one of the locations were to have a failure, there would be no interruption of access to the documents.	1 - Required							
STG.3.263	Storage	The system must contain an export tool for exporting of content in a non-proprietary format. This should supply both the document and the index values.	1 - Required							
STG.4.264	Storage	The system must support for State-supported, non-proprietary storage technologies, including NAS/SAN.	1 - Required							
STG.5.265	Storage	The system must have a data storage subsystem using commonly available / industry-standard file formats, file systems, and storage devices.	1 - Required							
STG.6.266	Storage	The system at a minimum must allow the archiving of documents to various media, including: <ul style="list-style-type: none"> • Windows file servers, to allow the leveraging of Share and NTFS permissions • Linux/Unix file servers • SAN/NAS/NFS Storage Devices 	2 - Preferred							
STG.7.267	Storage	The system must have the option to limit access to the storage locations based on service accounts; with functional permission granted by user role.	2 - Preferred							
STG.8.268	Storage	The system must have the ability to encrypt data at the database level and at the file storage level, as well as content that has been backed up/at rest.	2 - Preferred							

#	Requirement Area	Requirement	Priority	Offeror Proposed Solution	Out of the Box	Configuration Item	Customization Item	Extension/Interface	Other	Offeror Comments
STG.9.269	Storage	The system must support for flexible configuration and management of document storage structures.	2 - Preferred							
STG.10.270	Storage	The system must have a server storage subsystem which includes secure object path metadata, secure object store connectivity and the availability of volume-level data protection.	2 - Preferred							
STG.11.271	Storage	The system must support for data set management at a minimum: move, copy, delete, and reconfigure object store structures based on business needs.	3 - Optional							
STG.12.272	Storage	The system must allow users the ability to check documents out of the system for access via a localized copy that can be worked on, checked back in, and processed automatically.	3 - Optional							
STG.13.273	Storage	The system must allow content to be stored with pointers in the database storage, versus a blob in the database, for database backup granularity and performance	4 - If Available							
SYS.1.274	Scalability	System must support an unlimited number of customer-defined index value fields per document within one storage structure. These fields should be of various formats, including date, currency, alphanumeric, and numeric.	2 - Preferred							
SYS.2.275	Scalability	System must support multiple application and web servers in a load balanced configuration environment for redundancy.	2 - Preferred							
USR.1.276	User Experience	The system must have the ability to offer a rich-feature set of client-based solution functionality through a web deployable interface (i.e., rich internet application).	1 - Required							

#	Requirement Area	Requirement	Priority	Offeror Proposed Solution	Out of the Box	Configuration Item	Customization Item	Extension/Interface	Other	Offeror Comments
USR.2.277	User Experience	<p>This includes at a minimum the ability to execute ALL of the following DMS functions from a single screen:</p> <ul style="list-style-type: none"> • Index DMS stored documents using data on the business application screen, • Present user with a workflow step in context with the business application screen, • Launch a complete set of related documents presented in a tabbed folder view, • Launch scanning interface to perform ad hoc capture related to the account/record, • Create a scanning cover sheet with bar codes using data from the business application screen, • Retrieve documents based on a custom query from the business application screen, • Index captured documents using data from more than one screen within more than one business application, • Launch and complete an electronic form to track an event or start a workflow process, and • Create a form letter, based off of a Microsoft Word template, using data on the business application screen. 	1 - Required							
USR.3.279	User Experience	The system must provide the ability to display the document being indexed in a preview pane during the indexing process.	1 - Required							

#	Requirement Area	Requirement	Priority	Offeror Proposed Solution	Out of the Box	Configuration Item	Customization Item	Extension/Interface	Other	Offeror Comments
USR.4.280	User Experience	The system must have full client workstation support and client access from the following: Windows XP Professional SP2 or SP3, Windows 7 (32-bit and 64-bit), Windows 8 (32-bit and 64-bit), Internet Explorer 9.x or higher (Windows), Mozilla Firefox (Windows and Macintosh), and Google Chrome (Windows and Macintosh).	1 - Required							
USR.5.281	User Experience	The system must allow for other DMS functions to be performed, non-programmatically beyond retrieval, (i.e., point-and-click configurable), within the business application.	2 - Preferred							
USR.6.282	User Experience	The system must allow users to easily navigate and perform their primary job tasks with little formal training and with intuitive ribbon-style toolbars, tabs, and easy access features that are based on the familiar look and feel of Microsoft Office products.	2 - Preferred							
USR.7.283	User Experience	The system must have the ability for search an interface to accommodate multiple search methods from a single panel. This includes advanced search operators, full text searching, text searching, searches against notes, index value searches, searches against defined document types, all file formats, date ranges, etc.	2 - Preferred							
USR.8.284	User Experience	The system must have the ability to search and retrieve unstructured documents allowing users to search for multiple document types (e.g., text/archive, image, PDF, Word, etc.) in one search.	2 - Preferred							

#	Requirement Area	Requirement	Priority	Offeror Proposed Solution	Out of the Box	Configuration Item	Customization Item	Extension/Interface	Other	Offeror Comments
USR.9.285	User Experience	The system must have the ability to automatically cross reference related documents of similar or different file types to each other (e.g., a mainframe-generated text file to a TIFF image). If so, solution also provides the ability to identify hot spots or zones that trigger multiple related documents from the primary document.	2 - Preferred							
USR.10.286	User Experience	The system must have the ability for an integrated workflow experience that will provide task buttons and user interaction on a menu right from selected or open documents through standard document retrieval (i.e., user does not need to enter the Workflow Client).	2 - Preferred							
USR.11.287	User Experience	The system must have the ability for advanced full text search capabilities that include at a minimum: fuzzy, inflectional, thesaurus, proximity, wild card, and SOUNDEX.	2 - Preferred							
USR.12.288	User Experience	The system must have the ability for a ClickOnce deployable solution for the client interface, minimizing deployment and administration overhead and supporting IT policies.	2 - Preferred							
USR.13.289	User Experience	The system must have the ability for meaningful document names to appear in a search results list that can contain both static text as well as defined index values, offering a more detailed description of the documents returned.	3 - Optional							
USR.14.289	User Experience	The system must enable users (not administrators) to create their own personalized saved searches.	3 - Optional							
USR.15.290	User Experience	The system must have the ability to utilize full text searching alongside index value search. <i>Please provide a screen shot depicting this capability from a single interface.</i>	3 - Optional							

#	Requirement Area	Requirement	Priority	Offeror Proposed Solution	Out of the Box	Configuration Item	Customization Item	Extension/Interface	Other	Offeror Comments
USR.16.291	User Experience	The system must display all of the associated information about a document right alongside the image itself – displaying index values, notes, related documents, revisions, discussion threads, and document history.	3 - Optional							
USR.17.292	User Experience	The system must have the ability to retrieve and archive to the DMS system from the Microsoft Office toolbar and search and retrieve DMS stored content from directly inside the Microsoft Office application.	3 - Optional							
USR.18.293	User Experience	The system provides a dashboard component to create and manage personalized interfaces that present end users with access to priority content and tasks (e.g., workflow status report, commonly used document searches).	3 - Optional							
USR.19.294	User Experience	The system must provide the ability to auto-import camera images and media files directly from a connected device.	3 - Optional							
USR.20.295	Client	The system must allow the option for embeddable clients who can add document management system functions to the interfaces of third-party platforms and applications such as eCopy, Epic, ESRI, Lexmark, Xerox, Microsoft Office, and Microsoft SharePoint.	3 - Optional							
USR.21.296	User Experience	The system enables users to play, stop, and pause multimedia files (audio/video) with the native viewer.	4 - If Available							
USR.22.297	User Experience	The system must have the ability for a user to filter a broad search result list by selecting attribute fields (index values) on the demand.	4 - If Available							
USR.23.298	User Experience	The system must have the ability for users themselves to personalize the user experience (e.g., personalized home page that opens to personal workflow lifecycles, stored favorite retrievals, etc.).	4 - If Available							

#	Requirement Area	Requirement	Priority	Offeror Proposed Solution	Out of the Box	Configuration Item	Customization Item	Extension/Interface	Other	Offeror Comments
USR.24.299	User Experience	The system must have integrated tool to assess performance of client workstation hardware and network configuration directly from desktop.	4 - If Available							
USR.25.300	User Experience	The system must have integrated tool to track efficiency of key operations in the client from an end-user perspective, such as the time to open a document or route an item in workflow.	4 - If Available							
WEB.1.301	Web Services	The system must support web services-based data exchange with external applications over firewall-friendly HTTP or HTTPS with support for SSL and WS security standards per OIT Security Policies.	2 - Preferred							
WEB.2.302	Web Services	System must support API to allow integration with external applications on a variety of platforms via web services-based data exchange.	2 - Preferred							
WEB.3.303	Web Services	The system must allow external applications to retrieve documents or place them in the workflow process without invoking the document management system's user interface.	2 - Preferred							
WEB.4.304	Web Services	The system must allow development of external interactive applications based on web services standards such as SOAP, XML and WSDL, maximizing options for development environments and platforms.	2 - Preferred							
WEB.5.305	Web Services	The system must allow development of external interactive applications based on Web Services Interoperability (WS-I) standards, maximizing options for development environments and platforms.	2 - Preferred							
WEB.6.306	Web Services	The system must allow asynchronous messaging option for web services to reduce complexity of real-world integration projects.	4 - If Available							

#	Requirement Area	Requirement	Priority	Offeror Proposed Solution	Out of the Box	Configuration Item	Customization Item	Extension/Interface	Other	Offeror Comments
WEB.7.307	Web Services	The system must allow the option to initiate outbound web service requests to external applications and systems, and easily create and configure these services through the use of a user-friendly GUI.	4 - If Available							
WFL.1.308	Workflow	The system must allow users to use the document management system functionality independently of the workflow functionality.	1 - Required							
WFL.2.309	Workflow	The system must have the ability upon capturing a document to identify if it requires a workflow process.	2 - Preferred							
WFL.3.310	Workflow	The system must have a version control option that allows multiple users and groups to collaborate on documents with complete check-in/check-out privileges, version management, digital signing, and the ability to input comments for other users when doing check-ins and check-outs.	2 - Preferred							
WFL.4.311	Workflow	The system must support, out-of-the-box, the graphical design of workflows which utilizes a Business Process Modeling Notation (BPMN) compliant designer.	2 - Preferred							
WFL.5.312	Workflow	The system must have tools for annotating, or marking up, bitmap images for review, approval, or other processing purposes.	2 - Preferred							
WFL.6.313	Workflow	The system must support the ability of your BPMN compliant designer to produce (Business Process Execution Language) (BPEL) standard language.	2 - Preferred							

#	Requirement Area	Requirement	Priority	Offeror Proposed Solution	Out of the Box	Configuration Item	Customization Item	Extension/Interface	Other	Offeror Comments
WFL.7.314	Workflow	The system must provide preconfigured workflow reports that detail processing information including at a minimum: <ul style="list-style-type: none"> • Average Time to Process Document per Lifecycle, • Daily Workflow Usage, • Document Process Time per Workflow Queue, • Documents Processed per Queue, • Documents Resident per Queue, • High or Low Document Processing Identification, and. • Queue Processing Time per User in Minutes. 	2 - Preferred							
WFL.8.315	Workflow	The system must provide a workflow solution to native electronic application forms.	2 - Preferred							
WFL.9.316	Workflow	The system's electronic forms must at a minimum be architected in a way to interact with other parts of the DMS repository including at a minimum: <ul style="list-style-type: none"> • Document import capture, • Web (online form submission), • Web portal and SharePoint (form creation / submission through portal), • Index value design and structure, • Cross-referencing, • Notes/annotations, • Workflow (form auto-triggers a workflow process), and • E-mail (form viewed as attachment). 	2 - Preferred							
WFL.10.317	Workflow	The system must have the ability to incorporate native electronic forms. The system will provide for integrations with popular forms software like Microsoft InfoPath and Adobe LiveCycle to allow users to complete forms created with these products and processes them directly into the system repository.	2 - Preferred							
WFL.11.318	Workflow	The system must provide an integrated workflow environment.	2 - Preferred							

#	Requirement Area	Requirement	Priority	Offeror Proposed Solution	Out of the Box	Configuration Item	Customization Item	Extension/Interface	Other	Offeror Comments
WFL.12.319	Workflow	The system must have the ability to print and export graphical workflow diagrams.	2 - Preferred							
WFL.13.320	Workflow	The system must have the ability for full range of route types including at a minimum: sequential, sequential automatic, conditional, parallel, conditional parallel, inter-process routes, and automatic system queues.	2 - Preferred							
WFL.14.321	Workflow	The system must have the ability for a workflow queue type that contains a collection of distinct sub-queues which perform the same workflow function, reducing the number of alarms, routes and rules that are needed.	2 - Preferred							
WFL.15.322	Workflow	The system must have the ability to perform parallel processing by automatically routing a single document through multiple business processes simultaneously and allowing multiple users to access documents but does not allow concurrent editing.	2 - Preferred							
WFL.16.323	Workflow	The system must have the ability to support the use of electronic forms natively without requiring the purchase of any proprietary forms software.	2 - Preferred							
WFL.17.324	Workflow	The system must have the ability to route not only scanned paper but electronic objects such as email, faxes, PDFs, Office documents and more.	2 - Preferred							

#	Requirement Area	Requirement	Priority	Offeror Proposed Solution	Out of the Box	Configuration Item	Customization Item	Extension/Interface	Other	Offeror Comments
WFL.18.325	Workflow	The system must have the ability to present and access workflow from these devices and systems at a minimum: <ul style="list-style-type: none"> • BlackBerry, • iPad, • iPhone, • Windows Phone, • Droid, • Standard Client, • Outlook, • Web Client, • Business Application, • SharePoint, and • URL string. 	2 - Preferred							
WFL.19.326	Workflow	Offerors will need to adhere to State of Ohio OIT policy for eSignatures on DMS System.	2 - Preferred							
WFL.20.327	Workflow	The system must have the ability to create, define, and view relationships between folders.	3 - Optional							
WFL.21.328	Workflow	The system must have a workflow configuration and user interface environment that is integrated with the rest of the DMS solution.	3 - Optional							
WFL.22.329	Workflow	The system must have the ability to assign tasks, outside of formal workflow, which instruct a coworker or business partner to perform a document- or folder-related action such as signing, addressing document and folder deficiencies, or reviewing.	3 - Optional							
WFL.23.330	Workflow	The system must have the ability to group related documents in user-definable categories distinct from their index values in support of project organization and collaboration.	3 - Optional							
WFL.24.331	Workflow	The system provides reports utilizing custom transactions (i.e., approval time stamps added by a specific user during a transaction).	3 - Optional							

#	Requirement Area	Requirement	Priority	Offeror Proposed Solution	Out of the Box	Configuration Item	Customization Item	Extension/Interface	Other	Offeror Comments
WFL.25.332	Workflow	The system must have an integrated workflow environment providing rapid customization, configurable user privileges, and automated routing and alerts options, all in support of group collaboration.	3 - Optional							
WFL.26.333	Workflow	The system must have the capability to associate customizable electronic data collection forms with documents and folders in the system, to assist users in sharing information.	3 - Optional							
WFL.27.334	Workflow	The system must have customized instructions to be displayed within the workflow application, directing the end user on what functionality they can or should execute.	3 - Optional							
WFL.28.335	Workflow	The system must have the option to store a field of free-form text with each image, in support of group collaboration.	3 - Optional							
WFL.29.336	Workflow	The system must have the ability to maintain revision control on electronic forms to offer flexibility to display forms in their submitted state or with a new layout, allowing business processes to advance.	3 - Optional							
WFL.30.337	Workflow	The system must have the ability to structure workflow efficiently in support of staff absences, turnover and workload balancing.	3 - Optional							
WFL.31.338	Workflow	The system must have the ability to assign specific workflow process and queue management roles to defined users and groups.	3 - Optional							
WFL.32.339	Workflow	The system must have allow the interface for rapid drag-and-drop creation of system "shortcut" icons that are linked to and associated with distinct imaging system entities such as documents, batches, folders, workflow queues, and search queries.	3 - Optional							

#	Requirement Area	Requirement	Priority	Offeror Proposed Solution	Out of the Box	Configuration Item	Customization Item	Extension/Interface	Other	Offeror Comments
WFL.33.340	Workflow	The system must have the ability for the workflow process to interact directly with defined Web services, allowing external data received to be used as part of a workflow process (i.e., confirm a delivery date from a website such as ups.com). This is to be accomplished out-of-the-box with point-and-click configuration.	3 - Optional							
WFL.34.341	Workflow	The system must allow for the automatic distribution and sorting of work based on load balancing rules. Rules should include role, availability, percentage, order of arrival, index values, or the size of existing workloads for users, as well as custom- built work distribution rules.	3 - Optional							
WFL.35.342	Workflow	The system must provide a native, configurable workflow dashboard to monitor, in real time, the workload of end users. This should provide for an automatic visual notification within that dashboard when a process threshold has been crossed.	3 - Optional							
WFL.36.343	Workflow	The system must have the ability to copy and move workflow queues to easily facilitate workflow creation.	3 - Optional							
WFL.37.344	Workflow	The system must have the ability to configure “out of office” setting for workflow users, in support of document and other automated actions rerouting.	3 - Optional							
WFL.38.345	Workflow	The system must have the ability to capture information about workflow user actions and document routing - including at a minimum: the queues a document has been in, user interaction with the document, and additional relevant data for reporting.	3 - Optional							
WFL.39.346	Workflow	The system must have the ability to automatically perform time-based document removal actions from any workflow queue.	3 - Optional							

#	Requirement Area	Requirement	Priority	Offeror Proposed Solution	Out of the Box	Configuration Item	Customization Item	Extension/Interface	Other	Offeror Comments
WFL.40.347	Workflow	The system must have ad hoc shared document viewing, allowing one user to invite another user to simultaneously view a document on screen without first closing or putting document in workflow.	3 - Optional							
WFL.41.348	Workflow	Upon execution of a task within a workflow process, the proposed solution must provide the ability to automatically present a prompt requesting additional information for downstream processing (i.e., hiring manager determines a candidate as a “no fit” for a given position and is prompted for feedback on candidate’s positioning for a role elsewhere in the organization). This is to be accomplished out-of-the-box with point-and-click configuration.	3 - Optional							
WFL.42.349	Workflow	The system must have the ability for point-and-click interface for assigning users and groups to queues and defining detailed routing privileges.	3 - Optional							
WFL.43.350	Workflow	The system must have the ability to automate workflow routing based including at a minimum: defined index values, priority, creation time, and document type, length of time in queue, user/group who routed document, previous queue, document type, custom properties, and folder type.	3 - Optional							
WFL.44.351	Workflow	The system must have the ability to create workflow alarms that are centralized, reusable, and provide multiple notification methods.	3 - Optional							
WFL.45.352	Workflow	The system must have the ability to send messages to individual system users or all users currently logged on, directly from the server.	3 - Optional							

#	Requirement Area	Requirement	Priority	Offeror Proposed Solution	Out of the Box	Configuration Item	Customization Item	Extension/Interface	Other	Offeror Comments
WFL.46.353	Workflow	The system includes native capabilities to provide, or have partnerships for business rules engine, process modeling, process simulation, and process reporting.	3 - Optional							
WFL.47.354	Workflow	The system must have the ability to automatically set a document property based on its position in workflow.	3 - Optional							
WFL.48.355	Workflow	The system must have the ability to set queue-specific default destination queues for routed objects.	3 - Optional							
WFL.49.356	Workflow	The system must provide for a browser-based workflow dashboard to be displayed through provided interfaces, Microsoft SharePoint and WSRP 1.0 compliant portal products.	3 - Optional							
WFL.50.357	Workflow	The system should support Web Services for Remote Portlets Specification to enable content and application providers to access and provide services in a manner where they can be discovered and integrated with compliant portals without programming effort on the portal's side.	3 - Optional							
WFL.51.358	Workflow	The system must have the ability to use workflow independent of integration into business applications or leverage business application provided keys, links or pointers	3 - Optional							
WFL.52.359	Workflow	The system at a minimum must have the ability to create workflow alarms based on triggers such as number of documents in queue, defined index values, document type, and length of time in queue, custom properties, previous queue, and folder type.	3 - Optional							
WFL.53.360	Workflow	The system at a minimum must have the ability to dynamically display queue-specific workflow status, workflow alarms, and administrator messages on each client's workstation.	3 - Optional							

#	Requirement Area	Requirement	Priority	Offeror Proposed Solution	Out of the Box	Configuration Item	Customization Item	Extension/Interface	Other	Offeror Comments
WFL.54.361	Workflow	The system must have the ability to route documents and objects that are only partially indexed, by type of information or with partial details.	3 - Optional							
WFL.55.362	Workflow	The system must have the ability to create and apply custom scripts using a scripting language to automate queue actions on current, inbound, or outbound documents.	3 - Optional							
WFL.56.363	Workflow	The system must have the ability to create or utilize automatic system queues that perform a specific action on the items that are routed to them.	4 - If Available							
WFL.57.364	Workflow	The system must have the ability to send documents and folders into a specific workflow queue by dragging and dropping.	4 - If Available							
WFL.58.365	Workflow	The system must have the ability to assign tasks, outside of formal workflow, which instruct a coworker or business partner to perform a document- or folder-related action such as signing, addressing document and folder deficiencies, or reviewing.	4 - If Available							
WFL.59.366	Workflow	The system must have the ability to assign a series of task dependencies which can optionally be defined in a hierarchical manner	4 - If Available							
WFL.60.367	Workflow	The system must have the ability for drag and drop graphical workflow design tool.	4 - If Available							
WFL.61.368	Workflow	The system must have the ability to define, customize and view dynamically generated lists of workflow process and queue-specific documents, according to user-specified preferences.	4 - If Available							
WFL.62.369	Workflow	The system must have the ability to create advanced workflow logic using plain language, meeting many workflow objectives without scripting.	4 - If Available							
WFL.63.370	Workflow	The system must have the ability to use annotations on a document to drive routing.	4 - If Available							

#	Requirement Area	Requirement	Priority	Offeror Proposed Solution	Out of the Box	Configuration Item	Customization Item	Extension/Interface	Other	Offeror Comments
WFL.64.371	Workflow	The system must have the ability to link document index values to a host application within a queue or validate document index values while routing forward or back.	4 - If Available							

3.21. HRD Roll-Out Plan, Suggested Phasing

Offerors are to review the suggested phasing of scope, functionality and user groups with regard to the design, implementation and release of the proposed system. Should an Offeror choose to suggest alternative phasing as part of their proposal, any proposed alternates must include business justification, rationale and anticipated benefits of the proposed phasing strategy. Offeror proposals must include all elements of the below State suggested phasing. Absent Offeror recommendations to the contrary, and State acceptance of these recommendations, the following phasing shall prevail for the work in this Supplement.

3.21.1. Phase 1 – HRD and Pilot Agency Elements

- HRD
 - FileNET documents are migrated and indexed into the new DMS solution using the new index taxonomy.
 - Enable the full functionality of the DMS system for HR Records and participating agency HR Departments to capture, index, store, retrieve, and manage personnel documents.
 - Completed ePAR files with support documents are migrated and indexed into the new system.
 - Completed ePerformance files with support documents are migrated and indexed into the new system.
 - Daily migration and indexing of ePAR documents with supporting documents from OAKS HCM ePAR module to respective agency queue.
 - Daily migration and indexing of ePerformance documents with support documents from OAKS HCM ePerformance module to respective agency DMS queue.
- DAS Office of Employee Services (OES)
 - Paper documents to be captured and indexed by agency personnel as follows:
 - Current documents captured first.
 - Back files captured as needed.
 - System access to relevant ePAR and ePerformance documents.
 - Daily migration and indexing of ePAR and ePerformance documents to agency DMS queue.

3.21.2. Phase 2 Outside Agency Elements

- Paper documents to be captured and indexed by agency personnel.
- Current documents captured first.
- Back files captured as needed.
- System access to relevant ePAR and ePerformance documents.
- Daily migration and indexing of ePAR and ePerformance documents to agency DMS queue.

Agencies included:

- Paper-based HR departments,
 - Agriculture (AGR), and
 - Opportunities for Ohioans with Disabilities Agency.
- Existing document management system conversion:
 - Department of Medicaid.

3.21.3. Phase 3 Future Implementation for Outside Agency Elements

- Agencies with or without an existing DMS system can migrate and index existing documents to the new DMS system for the purpose of having seamless access to ePAR and ePerformance documents.
- Existing records will be migrated to new DMS solution using the new index taxonomy.
- System access to relevant ePAR and ePerformance documents.

- Daily migration and indexing ePAR and ePerformance documents to agency DMS queue.
- Future implementations will be defined per the Interval Deliverable Agreement requirements identified in the RFP.

3.21.4. Out of Scope

- EHOc Records will be accessed from their current environments; i.e. SLIM records from MS Access, HR2K, and OAK HCM Cognos Reports

3.22. Use Cases

3.22.1. On Boarding Process

- When employees onboard to a new agency, the agency must ensure there is a complete set of personnel documents to validate the employment process. The system therefore must identify all the necessary documents and indicate when the package is complete.

3.22.2. Employee Transfer

- It's a common practice for agency employees to transfer to another agency. The originating agency will initiate the transfer on the DMS. The agency will label which documents can be transferred to the new agency. The system will allow the new agency access to the existing records.
- DAS will have to develop, manage, and govern the index taxonomy for the DMS system for participants to use.

3.22.3. ePAR

- To change an employee's pay, benefit, or job status, the HR Department must initiate a Personnel Action form through the ePAR (Electronic Personnel Action Request) system. The ePAR system is a bolt-on application to the OAKS HCM system. When an ePAR is completed and approved the resulting PA PDF, supporting documents, and metadata needs to be transferred to the employee's PA Folder in the respective agency.

3.22.4. ePerformance

- All agencies are required to create, manage, and approved employee performance evaluations using the ePerformance application. The ePerformance system is a module on the OAKS HCM system. When an ePerformance evaluation is completed and approved the resulting PDF document, supporting documents, and metadata needs to be transferred to the employee's Evaluation Folder in the respective agency.

4.0 State Infrastructure, Operations Integration and Use Requirements

4.1. System Access: User Accounts

- Each user has a State of Ohio User ID and a password administered in a Microsoft Active Directory domain. A valid, active user ID and password must be utilized to access the system. The system will include a maintenance function for administrators to add, modify and inactivate user access for the system. The system will maintain the following data elements for the user account:
 - Username
 - User First Name
 - User Last Name
 - User Title
 - User Type
 - User Agency
 - User Email Address
 - Inactive?
 - Password
 - Date Added (read-only)
 - Date Modified (read-only)
 - User Last Modified (read-only)

4.2. Operational Requirements

- The system will be available except during scheduled maintenance and be designed to accommodate high usage will be during normal business hours of Monday-Friday 7am-6pm EST with no planned or unplanned outages during these hours.

4.3. Disaster Recovery & Backups

- DMS System data will be backed up using State backup devices by the State using Contractor provided scripts, backup target file systems or databases scripts and methods once each business day as to capture as many completed transactions as possible and to not impede State access to or use of the system.
- System data will be retained according to State data retention policy.

4.4. Policy Compliance

- The system will be compliance with State Security, Data Handling, IT and access Policies contained in Supplement 3 of this RFP.

5.0 Post Project Production Transition Requirements

Following the successful completion of Contractor System testing, and the support of State User Acceptance testing, the Contractor will support the Production release and go-live of the system.

The Contractor is to provide best practices in conjunction with the overall performance 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, and regression testing of performance testing items.

The Contractor will be responsible for working with the State and its 3rd party contractors, and executing the production deployment and roll-out of the PeopleSoft Technical Implementation to the Production Environment provided by the State.

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

- Execute required data conversions or migrations including, but not limited to, baseline PeopleSoft configuration tables and parameters, and ancillary supporting data as required by the system to function successfully in the production environment.
- Establish data to be used with the new solution by producing new data and reconciling and mapping different data and database representations.
- If required, convert electronic data into a format to be used by the new solution using the data conversion program.
- Perform required data matching activities and error reporting.
- Document data issues and provide to the State for resolution.
- Coordinate and confirm the State approval of data conversion results.
- Conduct production pilot(s) (including "day in the life" simulations) and fine tune solution as agreed appropriate.
- Compile and maintain solution issue lists.
- End to end final validation of the operational architecture for the system.
- Document activities, roles, responsibilities, tasks and procedures required to effectively operate and maintain the DMS system in the State Production environment. In addition to the activities, the plan must include, but not be limited to, staffing requirements by staff type and skill level, and the activities that must be performed by this staff.
- Develop, and thereafter maintain and make available to the State, a knowledge base of documentation gathered throughout the Project's life and allow for re-use of such documentation for future Projects.
- ★ Transition solution support responsibility to the Contractor Application and State OIT Infrastructure Managed Service teams as appropriate.
- Conduct a post-implementation review process upon the completion of the Project with the State's Project team, which will include an analysis of how the business system(s) resulting from the Project compare to the post-deployment performance requirements established for the Project.

- ★ Establish a performance baseline for the Project business systems, and where appropriate document requirements for future performance enhancement of the business systems implemented as part of the Project.

The Contractor will, as part of the migration to production operations of the final solution, perform and support the State in the following:

- **Implementation Assistance:** The Contractor must provide implementation assistance to State personnel assigned to this task. This will include the creation of implementation activity plans, implementation readiness checklists, and assistance to State users and managers who must perform tasks needed for successful implementation.
- **Implementation Certification:** The Contractor must provide an Implementation Certification Letter that certifies that the system is ready for implementation. The Certification letter must confirm:
 - All staff have completed staff and management training;
 - Be responsible for performing and verifying that all document and metadata has been migrated, validated, cleaned and accepted by the State;
 - Daily ingestion of HR images and documents, indexing and support documents processing have been met and are in place;
 - Help desk is established; and
 - All user and system supports are in place.
- **Implementation Report:** The Contractor, upon approval of the State Project Management Team, must implement DMS in accordance with the Contractor's approved implementation plan. The Contractor must produce an Implementation Report detailing all implementation activities and certifying that the system is operational and meets performance requirements.
- **Production Turnover:** Once the system has been approved, in writing, as ready for production, the Contractor must work with the State to perform a production turnover procedure. Among other things, this procedure requires the Contractor to turn over all system components in a systematic fashion into the production environment. The State will then ensure all compiled extension programs have corresponding source code and ensure that all programs are present. The State will also ensure that all components and modules of the production environment can be operated on-line or run to completion as appropriate, and that all modules, job streams (or scripts) are properly documented according to agreed upon standards. The Contractor must ensure that the source code, compiled modules (where required), job streams, other components of the production environment, and all documentation are ready and organized for the production turnover.

Contractor Deliverables

- ★ Implementation Plan (Repeats for each phase, as applicable).
- ★ Implementation Certification (Repeats for each phase, as applicable).
- ★ Implementation Report (Repeats for each phase, as applicable).
- ★ Production Turnover (Repeats for each phase, as applicable).

6.0 Application Maintenance and Applications Operations Requirements

The State's Office of Information Technology. Infrastructure Services Division (OIT/ISD) will be responsible for providing the infrastructure as a service to the Contractor for the operation of the system. In general, this service includes the following:

- Primary Computing Facility: State of Ohio Computing Center (secure Tier III capable facility)
- Alternate/Disaster Recovery Center: Ohio Based Secure Tier II facility

- Redundant Networking between State facilities and Data Centers (Metro-E to 10Gb/s via OARnet)
- Physical and Infrastructure Security Services
- Redundant Power, Cooling, Fire Suppression and onsite Redundant UPS/Power Generation
- Servers, Storage, Networking Devices, Firewalls, Security Appliances, Vulnerability and Virus Scanning to the operating system prompt

The State will provide ITIL based services in support of the Contractor as follows:

State Infrastructure Responsibility Matrix	
<p>Asset Management</p> <ul style="list-style-type: none"> ▪ Hardware Asset Tracking ▪ Software Asset Tracking ▪ Logistics Support ▪ Inventory Capture and Maintenance <p>Service Desk</p> <ul style="list-style-type: none"> ▪ Help Desk Operations ▪ Help Desk Tools ▪ Service Desk Processes 	<p>Enterprise Security Management</p> <ul style="list-style-type: none"> ▪ Emergency Response Service ▪ Threat Analysis ▪ Managed Intrusion/Detection/Prevention ▪ System Security Checking ▪ Security Advisory and Integrity ▪ Malware Defense Management ▪ Vulnerability Management ▪ ID Management ▪ Security Policy Management ▪ Security Compliance Support ▪ Security Audit
<p>Server Management</p> <ul style="list-style-type: none"> ▪ Platform Support (Tools/Processes Procedures) ▪ Unix/Intel Servers ▪ Incident Management ▪ Server Operations ▪ High Availability ▪ File Management <p>Storage Planning</p> <ul style="list-style-type: none"> ▪ Capacity Management ▪ Storage Performance Management 	<p>Data Center and Wide Area LAN/WAN Management</p> <ul style="list-style-type: none"> ▪ Enterprise Internet Services ▪ Regulatory/Change Management ▪ Network Engineering ▪ Standards ▪ LAN/WAN Management ▪ Network Operations and Management ▪ Network Capacity/Availability Management ▪ Network HW/SW Management ▪ Network Security ▪ Network M/A/C/D
<p>Data Center Architecture Planning</p> <ul style="list-style-type: none"> ▪ Hardware/Facilities Planning ▪ Unix/Intel Servers ▪ Platform Configuration Management ▪ Performance Management ▪ Capacity Management ▪ Batch Operations/Scheduling ▪ Storage Management ▪ Backup/Restore ▪ Media Management, Media Operations, Offsite Storage 	<p>Data Center Facilities Management</p> <ul style="list-style-type: none"> ▪ Site Maintenance and Operations ▪ Site Availability Management ▪ Routine Maintenance and Upgrades ▪ Non-Technical Services (parking lot, landscaping, snow removal etc.)

The Contractor will organize and provide the following Maintenance and Applications Operations services

6.1. Post Implementation and Long Term Support

On-site technical support and maintenance will be required after the acceptance the of the implemented Enterprise Imaging system. The on-site presence is essential to maintain a stable production environment, and to allow a smooth turnover of system responsibility to the State at the conclusion of the contracted services.

These services must include:

Production and Post Implementation Support: The Contractor must provide production support throughout the Project and post implementation support for a period of three months after the last implementation phase.

This post implementation support must consist of technical, functional, and operational support and must be provided by skilled Contractor personnel who have become familiar with the State over the course of the implementation effort.

In addition to the Project work requirements identified in this RFP, the State requires the selected Contractor to work with the State to produce fixed price costs and Deliverables for services per the Change Order processes identified in this RFP. The approach provides the State and the Contractor with the flexibility to set priorities and manage Deliverables for short-term efforts with potentially changing future and unanticipated requirements. The nature of this work would begin with post-implementation changes, modifications, and enhancements to the implemented DMS system.

6.2. Steady-State Operations and Maintenance Services (Run Services)

The Parties agree that the Steady State Operations and Maintenance Services under this Scope of Work will pertain to the period following the completion of the Transition of the supported computing environment to the Contractor to the completion of the contracted period, upon obtaining authorization from the State based on satisfying conditions of development and migration to production use. The Contractor will, through ongoing support and maintenance control processes, maintain support of the solutions developed by the Contractor during the term of the Contract. Such ongoing support and maintenance will include the following tasks and activities.

From time to time the State may have exceptional processing requirements (e.g., year-end close, end of year payroll processing, etc.) during which time no changes will be permitted to operational systems that may introduce unintended slow-downs, service interruptions or diminished service levels. During this period the Contractor is expressly prohibited from making any changes to a production environment with the exception of those changes as required to effect the restoration of service in a declared emergency or outage condition. The State will provide a schedule of these exceptional processing periods to the Contractor to aid in planning operations in consideration of these requirements.

6.3. Assist the State with Help/Service Desk Services Specific to the Solution

The Service Desk will provide the single point of contact (SPOC) for day-to-day communications between the State key personnel/IT staff and Application Administrators. Requests and incidents are reported by Users to the IT organization through the Service Desk in accordance with the Run Book or other supporting documents provisions. It is the single contact point for the State Users to record their problems and requests related to the supported servers and the Applications on those supported servers. If there is a direct solution, the Service Desk will provide immediate resolution, if not, then it creates an incident Report. Incidents will initiate the appropriate chain of processes: Incident Management, Problem Management, Change Management, Release Management and Configuration Management. This chain of processes is tracked using a trouble ticketing system, which records the execution of each process, quality control point, and store the associated output documents for traceability. Such processes and procedures will be as set forth in the Run Book or other supporting documents.

General Contractor tasks include:

- Handling incidents and requests through full life cycle management of all service requests as set forth in the Run Book or other supporting documents.
- Provide a Single Point of Contact for entry and exit to the service process and providing an interface for 3rd Parties essential to the service processes.
- Providing ease of use and a good customer experience for the State Users.
- Maintaining security and assuring data integrity as required in this SOW.

- Providing timely and effective communication which keeps the State Users informed of progress and of appropriate advice on workarounds.

The State will maintain a help desk designed to respond to user needs and inquiries and to the extent possible, resolve them with limited involvement from the Contractor. To the extent that the State help desk is unable to resolve technical or functional questions or issues from the user community, the Contractor will provide support functions as a service to the State help desk.

Contractor responsibilities include:

- To the extent incidents cannot be resolved by a centralized State Help Desk, tracking, monitoring, responding to requests and incidents and resolving incidents consistent with the established Service Levels and referring, as set forth in the Run Book or other supporting documents, requests to break/fix support resources for additional assistance;
- Providing documentation for the Contractor's development of or modifications to the system to help minimize transfers to specialized support;
- Providing the State with an updated list of Contractor-provided Support personnel or "on call" personnel who are responsible for system support, including contact phone numbers; and
- Working to correct environment defects or problems that require environment code or operational modifications.

The State will:

- Be responsible for all end-user training (hardware and software);
- For in-scope State-retained systems, provide systems status information to the Contractor Service Desk and updates as they occur. The Contractor will maintain such information as set forth in the Run Book or other supporting documents;
- Maintain and distribute a State contact list, including names and telephone, mobile/pager and fax numbers, for use by Contractor Service Desk staff to contact appropriate State personnel for problem determination assistance and escalation and ensure such personnel are available as required;
- Assist the Contractor in establishing call prioritization guidelines and escalation procedures;
- Ensure end-users have a basic level of understanding of the Contractor Service Delivery processes and adhere to such processes for accessing the Services;
- Communicate support responsibilities and procedures to the State Single Point of Contact and 3rd Party service providers (for example, providing call status and resolution to the Contractor Service Desk) and ensure adherence to such procedures;
- Assist the Contractor, as requested and in a time frame commensurate with the assigned problem Priority Code and associated Service Level commitment, in the resolution of recurring problems which are the result of end-user error;
- Resolve any of the State 3rd Party service provider performance problems affecting the Contractor's provision of the Services; and
- Be responsible for all the State 3rd Party support costs (for example, help lines or additional Application functional or technical support); and
- Be responsible for the resolution or closure of all calls related to products and services that are not within the Services.

6.4. Incident / Problem / Change (I/P/C, ITIL) Management

Under the ITIL service delivery model and as appropriate to driving a high quality service, the Contractor will:

- Provide the single point of IT contact for HRD support needs.
- Track and manage incidents by employing and implementing procedures for proactive monitoring, logging, tracking, escalation, review, and reporting (historical and predictive) of incidents, as set forth in the Run Book or other supporting documents.
- With the State, implement a process that establishes, to the extent reasonably possible, end-to-end responsibility and ownership of incidents in a manner that helps reduce redundant contacts and helps eliminate the need for the Users to describe the incident multiple times to different Contractor personnel.
- Categorize and document the relative importance of each incident according to the severity levels as agreed to by the Parties.
- Monitor and manage each incident, including incidents associated with changes, and report on the status of resolution efforts until it is corrected or resolved and an authorized User confirms such resolution, as set forth in the Run Book or other supporting documents.
- Ensure that all IPC tickets handled by the Contractor have sufficient detail as to understand the incident/problem or change requested, have timing to allow reporting as to start, stop and duration, include details as to the root cause and resolution to the problem and be structured in the Service Desk software to serve as the basis of applicable SLA reporting and service improvement statistical analysis;
- Assist the State with the prioritization and maintenance of outstanding work logs.

6.5. Additional Services

- To the extent an incident is due to errors or defects within an in-scope environment, supported server or in-scope software element licensed by a 3rd Party to the State, assist the State by referring such incident to the appropriate 3rd Party entity for resolution and coordinating with the 3rd Party contractor as appropriate to help minimize the State role in problem management.
- Performing trend analyses at the State request, and no less frequently on a quarterly basis when not otherwise requested, on the volume and nature of incidents in order to identify possible areas for improvement.
- Implementing measures to help avoid unnecessary recurrence of incidents, by performing root cause analysis and event correlation.

6.6. Job Execution / Production Control

The State maintains an operational “Run Book” to manage the scheduling of respective production operations, scheduled and routine jobs and reports. In general, these functions are executed on a daily, weekly and monthly basis co-incident with financial and human resources processing and close periods and Agency business cycles. The Contractor will assume this run book as part of operational responsibilities.

The Run Book will:

- Provide a high-level overview of the processes requiring State involvement (e.g., Change Management, Problem Management);
- Outline the current operating schedule for major production and operational schedules which include jobs, processing, report generation, interfaces and other regularly scheduled and routine tasks associated with the Offeror performing services in this area;
- Be used by the Contractor to provide the Services;
- Identify the Contractor/State interaction process interfaces; and
- Describe how the State and the Contractor will interact during the Term.

The Contractor must:

- Assign an individual to be the single point of contact to the State for the Run Book development and maintenance;
- Provide the proposed table of contents and format for the Run Book for the State review and approval;
- Develop and provide the draft Run Book, which will be customized by the Contractor to reflect the process interfaces (interaction between parties, roles responsibilities, timing and the like) between the State and Contractor;
- Review the State feedback and revise the draft Run Book to incorporate mutually agreed changes and regular optimizations;
- Upon request, communicate the Contractor's rationale for not including specific State comments or changes in the Run Book;
- Provide the final version of the Run Book to the State for its acceptance and approval, which will not be unreasonably withheld;
- Conduct process maturity assessments, identify process inhibitors, and propose process improvements to the State, as required;
- Jointly review the Run Book on a quarterly basis or more frequently, as required, and update and maintain the Run Book accordingly; and
- Provide appropriate Contractor employees with access to the Run Book, as required.

The State will:

- Assign an individual to be the single point of contact for the Run Book development and maintenance;
- Review and approve the proposed table of contents and format for the Run Book;
- Review and provide documentation containing the State's comments, questions and proposed changes to the draft Run Book;
- Request the Contractor's rationale for not including specific State comments or changes in the Run Book, as appropriate;
- Acknowledge receipt of the final version of the Run Book and provide acceptance and approval, which will not be unreasonably withheld;
- Identify process inhibitors and propose process improvements to the Contractor, as appropriate;
- Jointly review the Run Book on an quarterly basis or more frequently, as required; and,
- Provide appropriate State employees with access to the Run Book, as required.

6.7. Break/Fix Support

The Contractor will:

- Track, monitor and provide remediation for solution defects and incidents requiring system configuration or in-scope environment code or configuration changes;
- Identify and implement required system or configuration changes to address solution defects.
- Maintain solution documentation (technical specifications and testing documentation) as well as a compendium of common problems, root causes and remedy to aid in the identification and remediation of underlying system incidents;
- Test configuration changes to confirm resolution of defects;
- Identify, specify and system test (following OIT installation) 3rd Party supplied patches and fixes for 3rd Party supplied packaged systems software (including OS, BIOS, microcode, patches, service packs and similar), as well as new releases. If a new release contains new features and functionalities, the Parties may agree to

additional services required to enable or disable such features and functions (e.g., configuration, gap analysis, etc.) as part of any separate Project-related enhancement service;

- Support the State in performing applicable acceptance testing or review of any changes arising as a result of break/fix or patch/release Contractor responsibilities; and
- Ensure compliance with any State security mandated patches or system levels to the extent and system enhancement turnaround time required given the nature of the security mandate and report to the State in writing any risks or issues that the Contractor becomes aware of in providing Service to the State. For example: patches designed to address immediate or active Security issues may be scheduled for a near-real-time release, where other less pressing releases may be implemented during a scheduled maintenance or outage period.

6.8. Environment Technical Support

The Contractor will:

- Maintain environment performance, availability and stability of the production environments with the software resources and identify changes (if applicable) to the State for hardware or infrastructure resources.
- Identify to the State any issues that may adversely impact the State in-scope environment and operational requirements and that require analysis of the technical components of the system, including the applications, databases, ancillary and systems software and hardware.
- Conduct post-mortem reviews with the State for corrections to functional, integration or technical issues with in-scope environments or operations and incorporate resulting changes into ongoing continuous improvement initiatives.
- Upon the creation of any environment for State use, the Contractor will (unless excused in writing by the State) include these environments in regularly scheduled backup, maintenance, update/upgrade, patching, monitoring/reporting functions prior to productive use by the State and until the use of this environment is no longer required by the State.

6.9. System/Environment Administration Support

The Contractor will:

- For all Production, Non-Production (including environments that support systems development, testing, training, demo, QA and otherwise) Monitor environments, apply patches, and administer the system logs.
- Perform System technical activities including but not limited to: system code/object migrations, patch implementations, log administration, data copies and exports, interface and scheduled reporting/ETLs, and responsibility for incident resolution such that migrations into production will be executed at agreed periodic intervals and other production changes will be scheduled during the maintenance window.
- If required, support multiple release levels of System software/hardware elements for in-scope Services, provided that such support does not impair the Contractor's ability to meet the Service Levels until such time as all environments can be upgraded to the same patch/release level.
- Maintain an e-mail listing for each logical supported system resource. When the supported system resource has an unscheduled outage or reduction in required performance, the Contractor must notify the supported system user list based on outage/service reduction and promptly after supported server/service restoration in accordance with the Run Book or other supporting documents.
- Support and allow State access to the Contractor elements of the Service Desk system that contains all tickets managed by the Contractor for the State to use as it sees fit including providing estimate of time to complete, ticket prioritization and service restoration as well as all Service Level impacting items, whether State or Contractor initiated, in accordance with the Run Book or other supporting documents.

6.10. Systems Management and Administration

The Contractor will:

- Coordinate the installation, testing, operation, troubleshooting and maintaining of the Systems software.
- Identify and test packaging patches and other updates associated with supported Systems software, as well as supporting additional security-related fixes associated with the Systems software.
- Manage the security functions related to the Systems software including administrative access and passwords (i.e., users with root, admin, administrator, DBA or low-level read/write access) and the related security controls to maintain the integrity of the Systems software, based on the Contractor's standard service center security processes.
- Configure and maintain systems managed by the Contractor for network and remote access.
- Support the State in the maintenance of solution delivery elements including but not limited to advising, reviewing and testing of: software, microcode, patches, Systems software, connectivity software in accordance with the State policies listed in the State policies and have data and configuration currency adequate as to not delay testing effort or overall timing, unless otherwise requested by the State under an approved exception request.
- The Contractor will reasonably accommodate the State testing, review and approval processes prior to the installation of these elements in the production environment.
- Provide advisory services to support the following infrastructure services and roles:
 - Review supported server administration, set-up and configuration
 - Support performance tuning of infrastructure elements and perform performance tuning on system elements
 - Support infrastructure upgrades, updates or extensions
 - Support Infrastructure capacity planning
 - Support and Verify Backup and system restore operations performed by the State
 - Staff the Systems Management and Administration function at a sufficient level as to perform non-Production maintenance and administration functions in adherence to pertinent Service Level(s) and perform after hours updates to non-Production environments inclusive of code, data, patches, updates and other routine maintenance functions so that the entire imaging environment is consistent at all times following the application of maintenance elements.

The State will:

- Assist the Contractor in developing procedures for handling all planned and unplanned outages affecting the environment including review, approval, communication and proper documentation; and
- Notify the Contractor of any planned or emergency changes to the State's environment affecting the Contractor's provision of the Services.

6.11. System Environment Maintenance

The Contractor is to be responsible for all unit, system, performance and regression testing, as well as Installation Verification Tests (IVT) for system-related changes. Such changes must not be introduced into a Production environment until they have been through the complete test cycle in Dev/Test.

State personnel are responsible for all final, user-acceptance testing, including system, regression, performance testing, review of results and parallel testing in preparation for go-live.

The Contractor is responsible for monitoring all Third Party software vendors and vendor services for proactive notification of all applicable patches and updates. When new system impacting items are released they must be tested by the Contractor in its protected test environments, and jointly scheduled with the State for installation

during the next scheduled maintenance window. A priority update window may be required in advance of schedule if a patch or fix is deemed to be critical or security related.

Standard Contractor change control policies and practices will apply, and must follow the migration/test progression from Development to Test to Production.

The State does not require applying individual patches as they are released, unless there is a critical item that must be addressed in an “off-cycle” manner. The State’s required practice is to bundle up patches over the course of a specific period and then schedule those for application to the appropriate system environment per documented change control procedures.

The Contractor will test modified software prior to any move to production and coordinate with the State for scheduling and execution of end user testing of the service packs and patches. Acceptance testing signoff by the State is required prior to any move to a production environment.

6.12. Environment Management (Production, Development, System Testing/QA, , Demo/Train.)

The Contractor will:

- Perform environment/supported server tuning, code restructuring, and provide tools and other efforts to help improve the efficiency and reliability of environments and to help reduce ongoing maintenance requirements.
- Assess, develop, and recommend opportunities to reduce (or avoid) costs associated with environment support and operations.
- Provide appropriate Contractor-related data for periodic State analysis and review of resources deployed for preventive maintenance and planning preventive maintenance.
- Monitor and analyze trends to identify potential issues and follow-up on recurring problems.
- Maintain environments in accordance with the State strategies, principles, and standards relating to technical, data and Applications architectures as agreed-upon in this SOW, Projects, or the Run Book or other supporting documents.
- Install Systems software upgrades and enhancements for updates or revisions (i.e. 1.x, where x is the update/revision) as necessary to maintain the operability of the Services and implement technology changes (e.g., Systems software upgrades or new scheduling software). Included in the scope of such adaptive development work is testing new interfaces to Applications. The Contractor will install Systems software upgrades and enhancement for versions (i.e. X.1, where X is the version) as a Project approved by the State.
- Support the various service tiers (i.e., 11x5, 16x5, 24x7, compute processing (intermittent continuous operations on-demand)) production-availability schedule as agreed with the State and Authorized Users or in accordance with the Run Book or other supporting documents.
- Coordinate with designated State production staff, to manage production schedules.
- Update access and parameter or environment configurations contained within in-scope environments, where applicable.
- Establish a production calendar inclusive of daily and periodic maintenance activities.
- Generate and provide access to the State to daily production control and scheduling reports, including the production of monthly summary reports that track the progress of the Contractor’s performance of maintenance work.
- Provide timely responses to State requests for information and reports necessary to provide updates to the State business units and stakeholders.
- Implement and monitor the Management Services operations.
- Monitor operations for correctness and adherence to agreed quality, performance and availability criteria as set forth in the Run Book or other supporting documents.
- Perform batch monitoring and restart as follows:

- Verify batch jobs start as scheduled;
 - Monitor scheduled production batch jobs;
 - Resolve batch scheduling conflicts;
 - Monitor scheduler related incidents and develop and recommend changes to the scheduler database;
 - Schedule batch jobs, as requested by the State, that require expedited execution;
 - Notify the State as required in the Run Book or other supporting documentation; and
 - Perform job restart, as necessary, in accordance with resolution and restart procedures.
- Support production staff (both the State and Contractor) to create and adapt IT operational processes and procedures related to the in-scope environments.

6.13. Problem Management Services

Problem Management identifies and resolves the root causes of service disruptions. It includes:

- Root Cause Analysis and identification;
- Submission of Request for Change;
- Prioritizing resources required for resolution based on business need; and
- Updating the knowledge base.

Contractor responsibilities include:

- Analyzing trends and participating in the State continuous improvement process striving to enhance its operations and identifying continuous improvement ideas.
- Sharing applicable best practices that may improve the State processes and enabling technologies.
- Conducting periodic knowledge exchanges between Contractor team and the State designated individuals.
- Assisting with implementing the State defined IT control requirements including updating security matrix spreadsheets, and implementing Supported server and Systems software configurations for access control.

6.14. Service Reporting

The Contractor will:

- Provide the State with summary reports, on a monthly basis, to track the progress of the Contractor's performance on operations and maintenance work and provide access to daily operational reports or artifacts to confirm progress against agreed-upon operational and maintenance requirements and schedules as set forth in the Run Book or other supporting documents.
- Provide timely responses to State requests for information and reports necessary to provide updates to the State business units and end-user constituencies.
- For production or customer impacting incidents that result in a down System, or the unavailability of a production component, or a serious delay to the processing schedule, the Contractor must report progress based on the Service Level Agreement(s) in question until the issue is corrected or the State agrees that the issue causing the situation has been corrected. In all cases, the minimum reporting standard will be dictated by the Service Level Agreement for the impacted Services.

6.15. Maintaining Solution and Operations Documentation

Contractor will:

- Document the solutions developed or modified by the Contractor in accordance with established methods, processes, and procedures such that, at a minimum the State or a competent 3rd Party service provider can subsequently provide the same scope of Services following the period of Transfer Assistance Services.
- Develop and maintain, as agreed appropriate, the documentation on in-scope environments. Where it is determined that documentation is inaccurate (for example, due to demonstrated errors or obsolescence), and such inaccuracy may negatively affect the Services, Contractor will correct such documentation as part of normal day-to-day operational support.
- Update programmer, End User and operational reference materials.
- Maintain all documentation on the State's SharePoint site and ensure that all documentation is current following any change to the Service or System as it relates to documentation and conduct an annual audit for State review of all documentation to ensure ongoing compliance with these requirements.

7.0 Service Level Agreements and Contractor Fee Credits

7.1. Service Level Framework

This section sets forth the functional and technical specifications for the Service Level Agreements (SLA) and Service Level Objectives (SLO) to be established between Contractor and the State. This section contains the tables and descriptions that provide the State framework and expectations 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 detailed performance, management, and reporting requirements for all Contractor Service Services under this RFP.

Both the State and Contractor recognize and agree that new categories of Service Levels and Performance Specifications may be added during the term of the Contract as business, organizational objectives and technological changes permit and require.

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

Contractor will be required to comply with the following performance management and reporting mechanisms for all Services within the scope of this Statement of Work:

- **Service Level Specific Performance** – Agreed upon specific Service Level Agreements to measure the performance of specific Services or Service Elements. The individual Service Level Agreements are linked to Performance Credits to incent Contractor performance; and
- **Overall Contract Performance** – An overall performance score of Contractor across all Service Levels (i.e., SLA and SLO). The overall performance score is linked to governance and escalation processes as needed to initiate corrective actions and remedial processes.

7.2. Service Level Specific Performance Credits

Each Service Level (SL) will be measured using a "Green-Yellow-Red" (GYR) 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 financial credit will be due to the State (a "Performance Credit") 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.

The State believes, based on operating several very large scale systems under managed services agreements with a variety of leading industry vendors that these SLAs are aligned with the market, achievable under reasonable Contractor scope and effort considerations, and are specific, measureable and actionable for both the State and Contractor to measure performance and seek corrective actions. The State has chosen these levels in to be realistic and does not have the view that “generally green” future performance for a period of time does not excuse Vendor deficiencies that result in a red or yellow condition that impacts under a past operating condition State operations or service quality. Therefore **No Contractor recovery or “earn-backs” are permitted under this agreement.**

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. Except as explicitly stated in the Consecutive Months Credit table below, where a larger percentage may be at risk, Contractor agrees that in each month of the Agreement, up to 12% of the monthly recurring charges (MRC) associated with the Managed Services portion of this RFP (“Fees at Risk”). The Fees at Risk will pertain to failure to meet the Service Levels set forth in the Agreement.

The Contractor will not be required to provide Performance Credits for multiple Performance Specifications for the same event or incident, with the highest Performance Credit available to the State for that particular event to be applicable. For the avoidance of doubt, a single incident or event that may impact multiple SLA categories will only be calculated on a single SLA category that is most applicable to the incident or event and not multiple categories.

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 Contractor on the next scheduled or presented Contractor invoice to the State.

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

Contractor will not be liable for any 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 Contractor takes all steps to minimize the effect of such circumstances and to resume its performance of the Services in accordance with the SLAs as soon as possible.

The State requires the Contractor to promptly address and resolve Service impacting issues and to not have the same problem, or a similar problem reoccur in a subsequent month, therefore credit amounts shall escalate based on the following table:

Consecutive Months Credit Table (SLA Performance Credits)												
Individual SL GYR State	1 st Month	2 nd Month	3 rd Month	4 th Month	5 th Month	6 th Month	7 th Month	8 th Month	9 th Month	10 th Month	11 th Month	12 th Month
Red	A =1.50 % of MRC	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 = 1% of MRC	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									

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 aggregate Monthly Recurring Charge (the At-Risk Amount).

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

SLA Calculation EXAMPLE						
Monthly Recurring Charge (MRC) =		\$1,000,000.00				
Monthly At Risk Maximum Amount = 12% of MRC =		\$120,000.00				
Number of SLAs in Effect		8 (of 8)				
GYR State	1 st Month	2 nd Month		3 rd Month		
Red	0	\$ -	1	\$ \$15,000.00	1	\$22,500.00
Yellow	1	\$ 10,000.00	0	\$ -	1	\$ 10,000.00
Green	7	\$ -	7	\$ -	6	\$ -
Totals	8	\$ 10,000.00	8	\$ 15,000.00	8	\$ 32,500.00
Example Explanation	One SLA performing in Yellow State, 1% of MRC calculated		One SLA (different than month 1) performing in a RED State		Same SLA as Month 2 continues to perform in red State Another (different) in a yellow State	
Total Quarterly Credit: (month 3)	\$10,000.00 (month 1) plus \$15,000.00 (month 2) plus \$32,500.00 (month 3)					
Total Quarterly Credit:	to be credited on next scheduled invoice (or in the absence of an invoice at Contract End) a check to the State). \$57,500.00					

The total of any calculation factors may not exceed 100% of the total At-Risk Amount (i.e., fees at risk are capped at 12% of the value of a monthly invoice).

The Performance Credits available to the State under the terms of this document will not constitute the State’s exclusive remedy to resolving issues related to Contractor’s performance.

Service Levels will not apply during the Transition period, but will commence with the Contractor’s assumption of services in the production Steady State environment for all migrated elements in part or in full.

7.3. Treatment of Federal, State, and Local Fines Related to Service Disruption

Above and beyond the Service Levels discussed above, should any failure to deliver Services by the Contractor result in a mandated regulatory fine associated with late, incomplete, or incorrect filings as a **direct result of Contractor’s inability to deliver services under the defined Statement(s) of Work, production schedules, reporting and filing obligations, the requirements and Service Levels contained herein**, the Contractor will be obligated to issue a credit to the State equal to the amount of the fine.

7.4. 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 24 then Executive escalation procedures as agreed to by the parties will be initiated to restore acceptable Service Levels. The State may terminate the Contract for cause if:

- a) The overall SL score reaches a threshold level of 33 per month over a period of 3 consecutive months (equivalent to 75% of the service levels in a red State); or
- b) Contractor fails to cure the affected Service Levels within 60 calendar days of receipt of the State written notice of intent to terminate; or
- c) The State exercises its right to terminate for exceeding the threshold level of 44 in any month (all SLs missed) within five calendar days of receipt of Contractor's third monthly SLA status report.

Should the State terminate the Contract for exceeding the threshold level of 44 per month, it will pay to Contractor actual and agreed wind down expenses only, and no other Termination Charges.

The Overall Contract Performance under the terms of this document will not constitute the State exclusive remedy to resolving issues related to Contractor's performance.

The State retains the right to terminate for Overall Contract Performance under the terms of this Contract will apply only to this Scope of Work.

7.5. Monthly Service Level Report

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

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

Service levels specified herein shall be in full effect no later than ninety (90) days following the completion of migration of the current services and environments to the Contractor's responsibility. The Contractor agrees to:

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

7.7. Service Levels Review

Initial Review: Within six months of the Service Commencement Date or completion of Transition as outlined in this Supplement, whichever is sooner, the Parties will meet to review the initial Service Levels and Contractor's performance and discuss possible modifications to the Service Levels. Any changes to the Service Levels will be only as agreed upon in writing by the Parties.

Annual Review: Every year following the Service Commencement Date or completion of Transition as outlined in this Supplement, the Parties will meet to review the Service Levels and Contractor's performance in the period of time since the prior review and discuss possible modifications to the Service Levels. Any changes to the Service Levels will be only as agreed upon in writing by the Parties.

7.8. State Provided Service Support Infrastructure Elements

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

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

7.9. Imaging Managed Service: Service Level Commitments

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

Service Level		SLA or SLO	Coverage
1	Incident Resolution – Mean Time to Repair (Priority 1 Outages)	SLA	7x24
2	Incident Resolution – Mean Time to Repair (Priority 2 Outages)	SLA	7x24
3	Incident Resolution – Mean Time to Repair (Priority 3 Outages)	SLO	Business Hours
4	Service Availability – Application Availability	SLA	7x24
5	System Performance & Responsiveness	SLA	7x24
6	Incident Resolution - Issue Triage, Closure and Recidivist Rate	SLO	Business Hours
7	Security – Security Compliance	SLO	continuous
8	Monitoring & Auditing – Application Security Breach Detection, Notification and	SLA	7x24

Service Level		SLA or SLO	Coverage
	Resolution		
9	Job Schedule and Scheduled Reporting Performance	SLA	Scheduled Hours
10	Service Quality – System Changes	SLA	Scheduled Maintenance
11	Service Timeliness – System Changes	SLA	Scheduled Maintenance

7.9.1. Incident Resolution – Mean Time to Repair (Priority 1 Outages)

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

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

“Priority 1 Outage” is defined as :

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

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

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

Formula:

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

Measurement Period: Reporting Month

Data Source: Monthly Service Report

Frequency of Collection: Per incident

Service Level Measures:

Individual SL GYR State	Mean Time to Repair (Priority 1 Outages). Production Critical Environments	Mean Time to Repair (Priority 1 Outages). Non-Production Environments
Green	<= 4 hours	<= 8 hours
Yellow	> 4 hours and <= 6 hours	> 8 hours and <= 12 hours
Red	> 6 hours	> 12 hours

7.9.2. Incident Resolution – Mean Time to Repair (Priority 2 Outages)

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

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

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

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

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

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

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

Measurement Period: Reporting Month

Data Source: Monthly Service Report

Frequency of Collection: Per incident

Service Level Measures:

Individual SL GYR State	Mean Time to Repair (Priority 2 Outages). Production Critical Environments	Mean Time to Repair (Priority 2 Outages). Non-Production Environments
Green	<= 8 hours	<= 16 hours
Yellow	> 8 hours and <= 12 hours	> 16 hours and <= 24 hours
Red	> 12 hours	> 24 hours

7.9.3. Incident Resolution – Mean Time to Repair (Priority 3 Outages)

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

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

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

“Priority 3 Outage” Is defined as :

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

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

Inconsistency between non-production environment configuration (e.g., code, versions, patches, data, interfaces and other elements that comprise the non-production environment) with the then current Production Environment.

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

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

Measurement Period: Reporting Month

Data Source: Monthly Service Report

Frequency of Collection: Per incident

Service Level Measures:

Individual SL GYR State	Mean Time to Repair (Priority 3 Outages). Production Critical Environments	Mean Time to Repair (Priority 3 Outages). Non-Production Environments
Green	<= 5 business days	<= 7 business days
Yellow	> 5 business days <=7 business days	> 7 business days <=10 business days
Red	> 7 business days	> 10 business days

7.9.4. Service Availability – Application Availability

Business Intent: DMS is Available to All State HR Users for All Business Functions to Support Critical State HR processes

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

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

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

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

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

Measurement Period: Reporting Month

Data Source: Monthly Service Report

Frequency of Collection: Continuous, 24 hours a day

Service Level Measures:

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

7.9.5. System Performance and Responsiveness

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

Definition: System Performance and Responsiveness will be based upon an end-to-end service class performance baseline (e.g., network time, application/session response time, system time, and network return time) performed by the Contractor during the transition or as mutually agreed will perform for key service elements for a statistically valid sample of: 2 common transactions in each of Image Acquisition, Indexing, Workflow and Retrieval and Statistical Reporting and Data/Image Backup or Archive processes.

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

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

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

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

Measurement Period: Reporting Month

Data Source: Monthly Service Report

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

Service Level Measures:

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

7.9.6. Incident Resolution - Issue Triage, Closure and Recidivist Rate

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

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

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

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

Measurement Period: Calendar Quarter

Data Source: Incident Management System Report

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

Service Level Measures:

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

7.9.7. Security – Security Compliance

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

Definition: Security Compliance will be determined by monitoring compliance with the following five key performance indicators (KPI):

1. Compliance with the State IT security policies listed in Supplement 3
2. Update of antivirus signatures with most current version every 12 hours
3. 100% of DMS environments (inclusive of memory, disk and other file structures) to be actively scanned for viruses, Trojan horses, rootkits and other malware every 24 hours
4. 100% DMS devices actively scanned for open ports, forwarded ports or configurations not in keeping with adherence to the State security policies every 24 hours
5. 100% of environments to be reviewed for inactive/suspended user accounts every 30 days

Formula: Security Compliance =
$$\frac{\text{(Total number of individual KPI's performed per month) - (Total number of individual KPI's performed per month that were not in compliance)}}{\text{(Total number of individual KPI's performed per month)}}$$

(Total number of individual KPI's performed per month)

Measurement Period: Month

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

Frequency of Collection: Monthly

Service Level Measures:

Individual SL GYR State	Security Compliance
Green	99%
Yellow	N/A
Red	< 99%

7.9.8. Security – Monitoring & Auditing – Security Breach Detection

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

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

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

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

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

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

Measurement Period: Month

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

Frequency of Collection: Monthly

Service Level Measures:

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

7.9.9. Job Schedule and Scheduled Reporting Performance

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

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

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

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

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

Measurement Period: Monthly

Data Sources: Scheduled Job Report

Frequency of Collection: Daily

Service Level Measures:

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

7.9.10. Service Quality – System Changes

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

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

1. All System changes or updates (i.e., break fix, configuration, and patches) in any release to environments adhere to code and version control, contain written Contractor system testing and applicable performance testing results, contain back out/reversibility mechanisms prior to being presented to the State for authorization to release
2. System changes or updates (i.e., break fix, configuration, and patches) in any release to environments are implemented correctly the first time inclusive of all code, non-code, configuration, interface, scheduled job or report, database element or other change to the production environment
3. System changes or updates are propagated within 5 business days as mutually deemed appropriate to non-production environments such that environment configurations are synchronized and reflect the then current environment and a common development, testing, QA, demonstration and training environment is carried forward that is reflective of production
4. Production system changes (i.e., break fix, configuration, and patches) in releases that do not cause other problems
5. System changes or updates (i.e., break fix, configuration, and patches) in emergency releases are implemented correctly the first time that comprise the DMS system

Formula:

$$\text{Service Quality – System Changes} = \frac{\text{For Each System Change: Total Number of KPIs not met}}{\text{For Each System Change: Total Number of KPIs met}}$$

Measurement Period: Monthly

Data Sources: Production Change Report

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

Service Level Measures:

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

7.9.11. Service Timeliness – System Changes

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

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

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

Formula:

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

Measurement Period: Monthly

Data Sources: Production Change Report

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

Service Level Measures:

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

[this space intentionally left blank]

Supplement 2: Requirements and Statement of Work

Imaging Concepts and Proof of Enterprise Framework

State Enterprise Summary Opportunity

Financial Enterprise Processing Opportunity

Contents

Supplement 2: Requirements and Statement of Work	1
1.0 Solution Overview and General Scope	3
2.0 Citizen Data Conceptual Imaging Project	3
2.1. Citizen Data Systems Environment: Document Management Context	3
2.2. Citizen Data Requirements as “Proof of Enterprise Framework”	4
2.3. Citizen Data Imaging Conceptual Framework	5
2.4. Citizen Data Document Management Technology Capabilities	6
2.5. Citizen Data Electronic Form Storage Capabilities	7
2.6. Citizen Data System Support for Scanning and Storage of Imaged Documents	7
2.7. Citizen Data System Imaging Capabilities: Searching of Documents	7
2.8. Citizen Data Requirements Matrix	8
2.9. Conceptual Citizen Data Solution Requirements Matrix	9
3.0 Financial Document Processing: Conceptual Imaging Project	13
3.1. PeopleSoft Financials Requirements	13
3.2. Integration Requirements	14
3.3. Process Overview and Imaging Requirements	14
3.3.1. Inbound Paper Mail Process	15
3.3.2. Agency Document Upload	15
3.3.3. Agency Email Upload	16
3.3.4. Agency Fax Upload	17

1.0 Solution Overview and General Scope

The State, via more than 120 Agencies, Boards and Commissions has a variety of requirements that are fulfilled by imaging/workflow/integration solutions that are specific or related to the business needs of the State and aligned with the missions of each Agency, Board and Commission. State Agencies maintain a set of emerging near term imaging and workflow requirements associated with large scale systems integration projects where the focus of the data contains Citizen Data. In addition, most large Agencies process some form of high volume imaged based set of financial transactions (invoices, receivables, payments, contracts etc.)

While the State is initially implementing the imaging solution for HRD (under Supplement 1 of this RFP) as a “proof of the framework’s” applicability to these and other Enterprise level imaging requirements, this Supplement contains representative work, requirements, integration and conversion considerations that the State will use to validate the Enterprise applicability of the Offeror proposed solution.

In general, a State Agency was chosen to understand the considerations regarding the acquisition, management, processing and protection of private Citizen Data (generally protected under HIPPA) and the financial transaction information arising from businesses in the State of Ohio.

The State seeks to identify such a solution via this RFP to:

- Serve as a basis for ongoing standardization for other systems requirements;
- Provides an extensible enterprise platform that is “image source” and “target system” integration agnostic;
- Flexible and extensible to address high volume imaging, transaction processing, storage, retrieval and integration requirements of any Agency, particularly those of Citizen and Financial oriented data; and
- Can be implemented in a modular fashion that allows the State to leverage existing investments and deployments in scanning technology and services, workflow, document management, storage, networks and open systems based on modern APIs and integration format capabilities.

Each of the Citizen Data and Financial Opportunities will be presented in turn and in summary.

2.0 “Citizen Data” Conceptual Imaging Project

2.1. Citizen Data Systems Environment: Document Management Context

The State has contracted with a variety of vendors to design, implement and operate systems to manage the State’s delivery of Citizen Data and services to the public.

These systems manage all transactions, eligibility, enrollments, reporting and other functions associated with administering Citizen Data programs and as such have a significant document management, imaging, workflow and other requirements that are germane to a vendor provided Enterprise solution and somewhat aligned with the aforementioned HRD requirement set in Supplement 1.

In general, the Citizen Data system has provision to accommodate:

- Storage of Electronic Forms
- Scan and Store Imaged Documents
- Searching of Documents
- Digital Rights Management Capabilities

State systems are being designed to support and improve workflow efficiency through the use of a single logical repository for recipient and applicant documents and leverages integration a variety of commercial off the shelf packages. For this summary opportunity, Offerors should assume that the base integration will be with the Oracle WebCenter Content (OWC) product to provide a solution for the State's content management needs.

Offerors are to note that the State has no preference, nor endorses any particular vendor's product, and that the Oracle suite was chosen as a common denominator that is generally understood in the industry and has published integration standards.

The State solution allows documents, when applicable, to be shared amongst programs. Document sharing capabilities are designed to increase the accuracy and timeliness of eligibility application processing, with shared access to documents such as birth certificates, pay stubs, drivers licenses, etc.

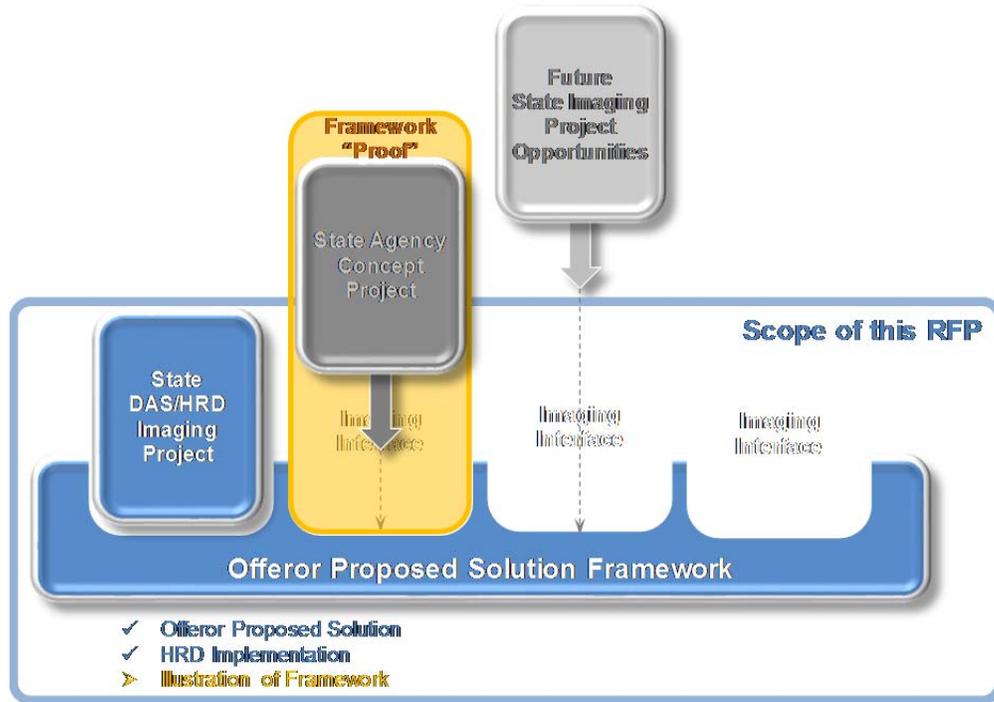
OWC is used in the system to increase the efficiency of their administrative, case-related functions and provides the ability to easily transfer case files between case managers from one county to another. As a result of this integration of OWC into the contracted system, a system where case documents are added to the online document repository, which facilitates the sharing of documents between case workers located in different counties.

The State architecture and the integrated OWC solution is designed to reduce the risk and cost associated with a variety of regulatory and legal compliance processes, including International Organization for Standardization (ISO), the Citizen Data Insurance Portability and Accountability Act (HIPAA), Federal Drug Administration (FDA) 21 CFR Part 11, and Six Sigma.

2.2. Citizen Data Requirements as "Proof of Enterprise Framework"

As a goal of this RFP is to identify a suitable framework for use with various State Enterprise requirements, the State has identified a near term conceptual project by which to evaluate the Offeror's proposed enterprise imaging and document management framework through the consideration of Citizen Data general requirements. Conceptually, these requirements are not as specific as the HRD requirements contained in Supplement 1, nor will further details be made available to Offerors during the inquiry period to this RFP. Offerors are to consider these conceptual requirements and indicate, using the proposed HRD solution, the approach, scope, framework coverage and other features and functions that are part of the proposed solution and how they (as a framework) would map to addressing Citizen Data requirements. The response to these requirements will be factored as part of compliance with the State's Enterprise framework requirements as further described elsewhere in this RFP. Using the conceptual framework established in Section 1 of this Supplement, the work can be viewed as follows:

Conceptual Project: Citizen Data Imaging Support

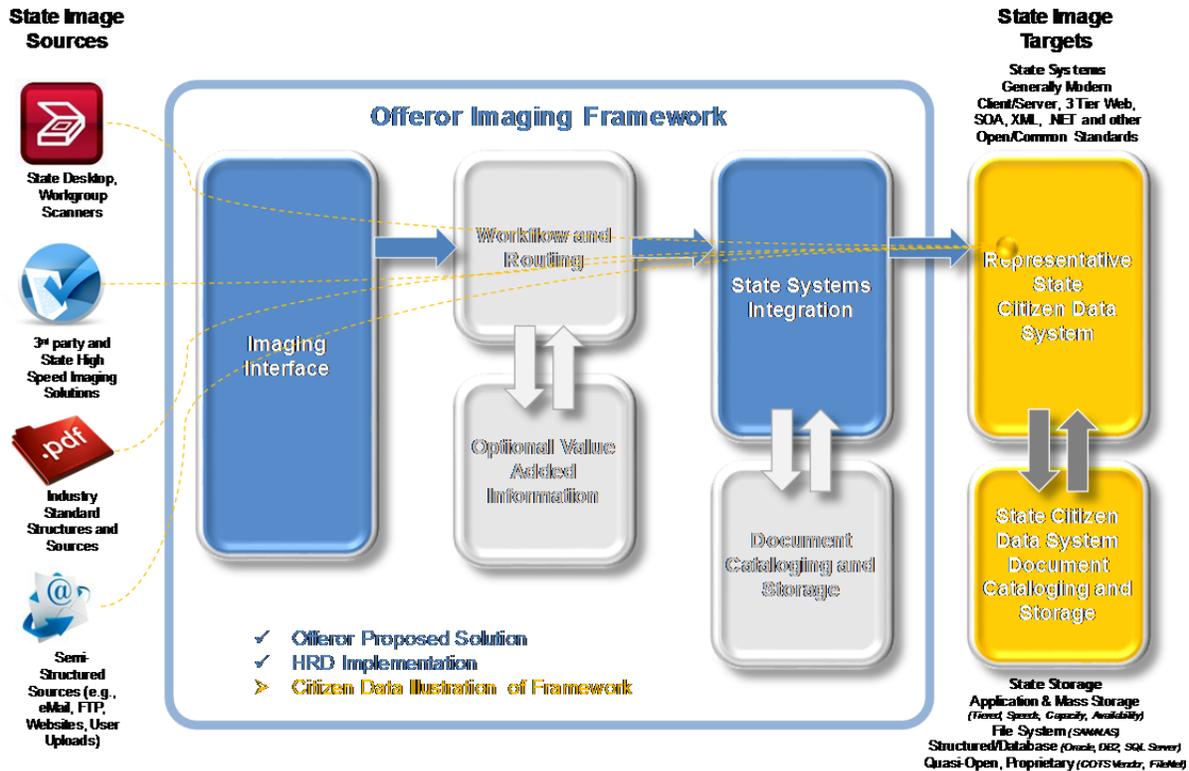


2.3. Citizen Data Imaging Conceptual Framework

The State's Citizen Data solution has extensive provisions for accepting, searching and managing a variety of applicant and participant images via interfaces and software technology elements, however the image acquisition, verification, general workflow and integration with the Citizen Data solutions have not been specified or identified in any granular detail.

Based on the requirements contained herein, Offerors are encouraged to share as many details as to similar business challenges and requirement sets in a variety of Citizen Data domains as to the potential challenges, business benefits, technology, functional and business process enablers or capabilities contained or addressed by the proposed solution for the HRD imaging project as they could be extended to incorporate Citizen Data emerging needs. As a conceptual framework for these requirements, the framework established in Section 1 of this Supplement are again used to orient Offeror's to the State's potential needs and requirement set as follows:

Conceptual Organization of Solution Requirements: Future Opportunities



Elements pertaining to the potential Citizen Data project are highlighted in orange text and graphics in the above diagram.

2.4. Citizen Data Document Management Technology Capabilities

The OWC document management solution is designed to effectively and efficiently capture, secure, share, and distribute digital and paper-based documents and reports. OWC provides the governance and auditing capabilities needed to minimize the risks and costs associated with regulatory and legal compliance.

The Ohio Citizen Data portal applications including the Citizen Data solution accesses the OWC's document management functionality via the Citizen Data shared Content Management Service. The solution also uses Adobe Lifecycle forms and the notification engine included in the Citizen Data solution suite. OWC is integrated with the Citizen Data for integrated retrieval of case documents. The solution also includes Oracle WebCenter Content for document capture. It provides the State a COTS based capture tool for transforming paper into digital content.

Oracle WebCenter Capture is integrated with OWC to provide one system to capture, store, manage and retrieve citizen critical business content. This solution allows Citizen Data agencies to effectively capture all types of digital and paper-based content, store the content in a centralized system, control access permissions to the content, and preserve or dispose of the content based on State specific content lifecycles. Via this solution, the State Citizen Data agencies can effectively manage different types of content, regardless of format, location where it is stored, or retention and archiving policies. As OWC integrates with capabilities in desktop applications such as Microsoft Word and Excel, OWC gives users a choice of different in-context interfaces, including web browsers, Microsoft Windows Explorer, and Microsoft Outlook.

2.5. Citizen Data Electronic Form Storage Capabilities

Several State Citizen Data systems provide for integrated client correspondence, notifications and forms process. As part of these processes, State Citizen Data systems provide the shared Forms Service and Correspondence Service to support the integration between Ohio portal applications and the underlying Forms Management solution provided by Adobe.

After generation, forms and notices are stored within the OWC repository. Each piece of correspondence is labeled with the date it was generated, the document name, and the status of the document, including the method of distribution. The State Citizen Data systems (in general) support the generation of notices in multiple formats and distribution of these notices through email, print, web (including social networking media) and mobile devices provided by the Adobe forms management tool.

2.6. Citizen Data System Support for Scanning and Storage of Imaged Documents

State Citizen Data systems are designed to support authorized Agency users access of electronic forms to make informed decisions on the appropriate services to offer citizens and applicants. Oracle WebCenter Content's imaging together with Oracle WebCenter Capture and Oracle WebCenter Forms Recognition provides an imaging platform for end-to-end management of document images within transactional business processes. OWC provides comprehensive content management and business process management capabilities - from document capture and recognition, to imaging and workflow.

After generation, forms and notices are stored within the OWC repository. Each piece of correspondence is labeled with the date it was generated, the document name, and the status of the document, including the method of distribution. The system generates notices in multiple formats and distribution of these notices through email, print, web (including social networking media) and mobile devices.

In addition, the State's online portal is integrated and supports client-initiated document uploads and connection with online cases. Documents scanned and stored are placed into the OWC document repository and made available to the appropriate Citizen Data users.

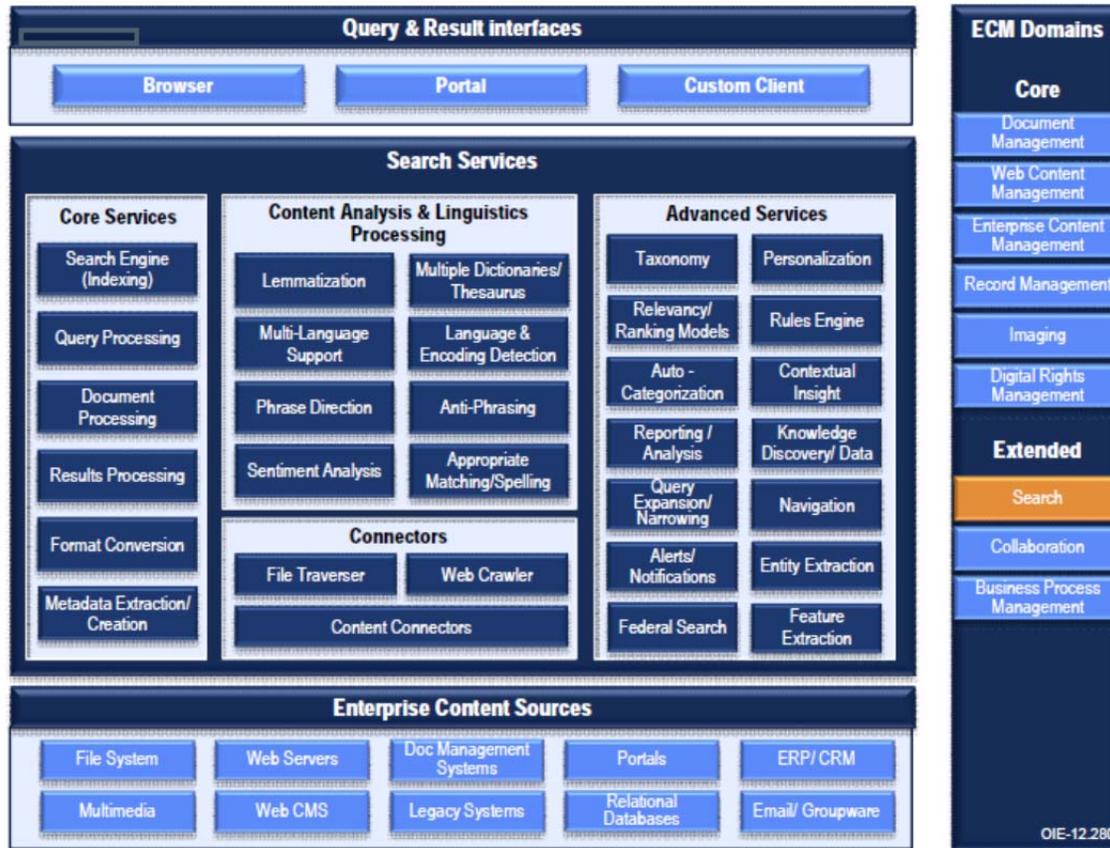
2.7. Citizen Data System Imaging Capabilities: Searching of Documents

Ohio's Citizen Data application can upload, retrieve and search imaged documents using the shared content management and enterprise search services functionality via a SOA component. When performing a document search, the most likely hits and exact matches are displayed on the top of the search result page, with other possible matches below, in descending order.

As part of enterprise search capabilities the State of Ohio is provided a secure, high quality, easy-to-use search function across enterprise information assets. The OWC search capabilities include content analysis and advanced services to provide Agencies with an enterprise search service across multiple content sources, in addition to the OWC document repository.

Additionally, the OWC metadata search capabilities allow users to use parameterized searches. By applying metadata, users can narrow the search to particular values—documents of a certain file type, authored by a specific individual, within certain dates, with specific keyword, etc.

Citizen Data System: Conceptual Capabilities Map



2.8. Citizen Data Requirements Matrix

The State has developed a set of functional requirements contained in the next section of this supplement pertaining to Citizen Data solution needs. To assist the State in reviewing the Offeror's response, the Offeror proposed solution or tools in satisfying these requirements and understand the implementation scope, approach and dependencies that will be in effect for the implementation and ongoing operation and maintenance of the Offeror solution, Offerors will complete the Requirements Matrix as follows:

Offeror Proposed Tool/Solution	Offerors are to include the name and major version number of the Proposed Tool/Solution to address the requirement (e.g., Acme Corporation® WidgetMaster™ v9.1)
Out of the Box	Offerors are to indicate, in full lifecycle development hours (i.e., design, implement, test), the number of hours to be spent implementing this requirement using as delivered functions of the Offeror proposed solution. Should this not be applicable, Offerors are to record a zero (0) in this column.
Configuration Item	Offerors are to indicate, in full lifecycle development hours (i.e., design, implement, test), the number of hours to be spent implementing this requirement using as configurable functions (e.g., interfaces, reports, workflows, screen elements) of the Offeror proposed solution. Should this not be applicable, Offerors are to record a zero (0) in this column.

Customization	Offerors are to indicate, in full lifecycle development hours (i.e., design, implement, test), the number of hours to be spent implementing this requirement using as configurable functions (e.g., interfaces, reports, workflows, screen elements) of the Offeror proposed solution. Should this not be applicable, Offerors are to record a zero (0) in this column.
Extension/Interface	Offerors are to indicate, in full lifecycle development hours (i.e., design, implement, test, deploy etc.), the estimated number of hours to be spent implementing this requirement using as extensions or interfaces (e.g., interfaces, reports, workflows, screen elements) of the Offeror proposed solution to a SOA based conceptual Citizen Data system, interfaces, or other Offeror provided solution elements. Should this not be applicable, Offerors are to record a zero (0) in this column.
Other	Offerors are to indicate, in full lifecycle development hours (i.e., design, implement, test), the number of hours to be spent implementing this requirement using as that do not fit into the aforementioned categories. Should this not be applicable, Offerors are to record a zero (0) in this column.

For the avoidance of doubt, all Offeror proposed hours for the effort, absent Project Management and Client administration and production migration associated with compliance with State requirements must be included in the provided Requirements Matrix.

2.9. Conceptual Citizen Data Solution Requirements Matrix

The following is the listing of Conceptual Citizen Data solution requirements in their entirety. The State has prioritized the functional requirements based on current need as follows:

1 - Required	Mandatory requirements that the Contractor must include in their proposal, design, implement and test and support the production use of in their response
2 - Preferred	Requirements that the State believes are dependent on implementation of Must Have requirements should be included based on scope, timing, cost and integration considerations
0 – Available for Use / Integration	Based on the State’s implemented Citizen Data Solution capabilities, these features and functions are available for use, integration or part of the Offeror’s proposed conceptual solution to demonstrate the flexibility and use of the Offeror Proposed solution for other State enterprise needs.

Offerors must complete the table as provided and not make any alterations to any rows or columns that have a **blue** column label which represent the State’s base requirement and priority. The State requires an Offeror response to all **green** column label cell contents.

For convenience, a Microsoft Excel based version of these requirements are contained in the RFP Exhibit library.

Requirements Matrix Follows

#	Requirement Area	Requirement	Priority	Offeror Proposed Tool/Solution	Out of Box	Configuration Item	Customization	Extension/Interface	Other	Offeror Comments
Citizen Data-01-01	Capture/Scanning	The system must be able to receive/scan, catalogue and store documents and materials received as well as integrate within the system workflow.	1 - Required							
Citizen Data-01-02	Store and Retrieve	The system must index and maintain version history of documents. Additionally, indexing needs to be taken into consideration.	1 - Required							
Citizen Data-01-03	Universal View	The system must provide a shared 'Common Area' for cases that can be accessed across various Workers, across all Counties and across various systems. This allows for a universal view that can be applied to all programs administered within the Ohio Conceptual Citizen Data System, as well as communicates with other programs administered outside of this system.	1 - Required							
Citizen Data-01-04	Business Process Lifecycles	The system must allow for the incorporation and standardization of business processes tied to specific activities and functions.	1 - Required							
Citizen Data-01-05	Version history management and tracking	The system must have the capability to track and view the version history of documents. Ideally documents would be able to be edited with proper controls in place.	1 - Required							
Citizen Data-01-06	Notifications	The system must provide notifications built into the system to inform both residents and Workers when something in the system has changed and impacts a resident's eligibility determination.	1 - Required							
Citizen Data-01-07	Auto-Fill Forms	The systems must allow for forms to be auto-filled with information from the system	2 - Preferred							
Citizen Data-01-08	Forms Management	Forms management needs to be centralized across the State and managed through the system. While managed at the State level, the capability for Counties to manage sub-categories of forms at the local level would be required to accommodate for needs at the local level.	2 - Preferred							
Citizen Data-01-09	Redaction	The system must have the capability to redact and update forms within the system and not only create notes to highlight updates.	2 - Preferred							
Citizen Data-01-10	Customizable Security Levels	The system must allow for the creation and customization of security levels with the system.	2 - Preferred							
Citizen Data-01-11	Reports	The system must allow for the production of standardized reports related to performance and workflow metrics.	2 - Preferred							
Citizen Data-01-12	Confidentiality Tagging	The system must allow for the customized need to accommodate confidentiality tagging to prevent abuse of access within the system.	2 - Preferred							
Citizen Data-01-13	Online Web-based Access	The system must allow for an authorized user to view documents and materials within the imaging solution remotely and online.	2 - Preferred							
Citizen Data-01-14	Appointment Scheduling	The system must accommodate and allow appointment scheduling, particularly for workforce interviews. Additionally, scheduling should interface with centralized forms for notification purposes.	2 - Preferred							
Citizen Data-01-15	Audio and Electronic Signatures	The system must allow for capturing audio and electronic signatures electronically (essential when providing the capability for residents to apply via phone applications for all programs)	3 - Optional							

#	Requirement Area	Requirement	Priority	Offeror Proposed Tool/Solution	Out of Box	Configuration Item	Customization	Extension/Interface	Other	Offeror Comments
Citizen Data-01-16	Seamless automated mailing process	The system must allow for a seamless automated mailing process that that can push out mail/forms through a central mailroom by clicking a single button.	3 - Optional							
Citizen Data-01-17	Screen pop	The system must allow for "Screen pop"(when a resident calls in, their case automatically appears on the Agency Worker's computer screen)	3 - Optional							
Citizen Data-01-18	Bar-Coding	The system must incorporate bar-coding as a primary means of tracking and auto-indexing documents. The users of the systems should be able to manage how bar-coding is used and direct the system to take action based on direction from the systems users.	3 - Optional							
Citizen Data-01-19	Right Fax & Email	The system must have the ability to fax and email forms directly from the system.	3 - Optional							
Citizen Data-01-20	Records Retention	The system must allow for customized storing and purging of documents based on a standard or designed period of time.	3 - Optional							
Citizen Data-01-21	Citizen Data System Capabilities	The solution shall provide built-in viewers/converters for a wide variety of file types	0 - Available for Use/Integration							
Citizen Data-01-22	Citizen Data System Capabilities	The solution shall provide digital rights management capabilities	0 - Available for Use/Integration							
Citizen Data-01-23	Citizen Data System Capabilities	The solution shall provide check In/check out functionality for electronic documents	0 - Available for Use/Integration							
Citizen Data-01-24	Citizen Data System Capabilities	The solution shall provide notification features for files that are checked out (overdue, availability, etc.)	0 - Available for Use/Integration							
Citizen Data-01-25	Citizen Data System Capabilities	The solution shall ensure version control of documents as they are changed or modified	0 - Available for Use/Integration							
Citizen Data-01-26	Citizen Data System Capabilities	The solution shall allow rollback to a previous version of a document	0 - Available for Use/Integration							
Citizen Data-01-27	Citizen Data System Capabilities	The solution shall enable collaborative document creation and/or markup	0 - Available for Use/Integration							
Citizen Data-01-28	Citizen Data System Capabilities	The solution shall enable attachment of documents to e-mails and e-mail distribution lists	0 - Available for Use/Integration							
Citizen Data-01-29	Citizen Data System Capabilities	The Solution shall utilize the solutions authorization and access control for file level security	0 - Available for Use/Integration							
Citizen Data-01-30	Citizen Data System Capabilities	The Solution shall have the ability to, based on rules or context, automate the creation of indexing, meta data and overall taxonomy	0 - Available for Use/Integration							
Citizen	Citizen Data	The solution shall have robust bulk load and conversion features	0 - Available for							

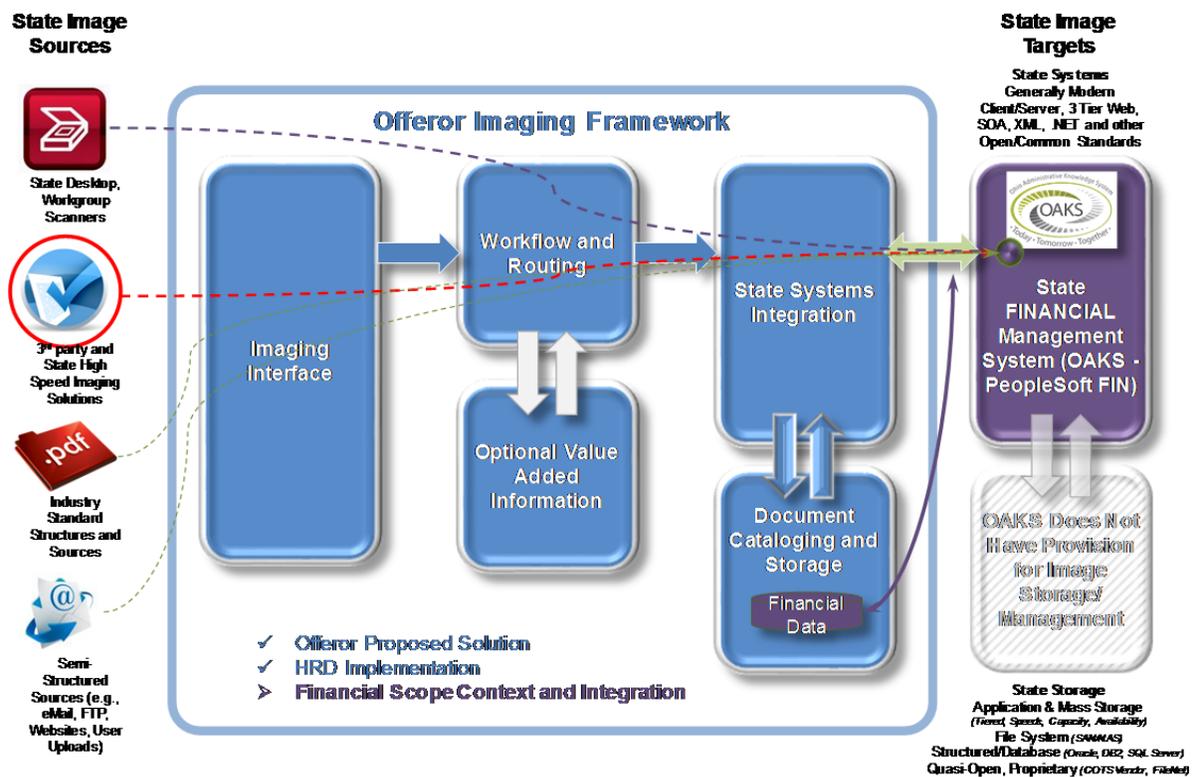
#	Requirement Area	Requirement	Priority	Offeror Proposed Tool/Solution	Out of Box	Configuration Item	Customization	Extension/Interface	Other	Offeror Comments
Data-01-31	System Capabilities		Use/Integration							
Citizen Data-01-32	Citizen Data System Capabilities	The solution shall provide a configurable, intelligent, accurate and scalable data extraction feature	0 - Available for Use/Integration							

3.0 Financial Document Processing: Conceptual Imaging Project

The State maintains a variety of imaging and financial transaction processing locations that are designed and managed both centrally - for common transactions and functions) as well as within Agencies – that are specific to the needs of the Agency, Agency systems and transaction requirements. A common financial platform for the State is The Ohio Administrative Knowledge System (OAKS) which, in general processes accounts payable, inter-state transfers of funds and transactions, and vouchers. For ease of Offeror response, an OAKS orientation is included in this conceptual project. OAKS is based on PeopleSoft Financials 9.2 and should be the focus of the Offeror response that demonstrates the capabilities, features/functions and Enterprise fit for this example under the following requirement set.

Conceptually, using the established framework used elsewhere in this RFP, this can be viewed as follows:

Conceptual Project: Finance Imaging Support



3.1. PeopleSoft Financials Requirements

This solution will be fully integrated/interfaced with the PeopleSoft Financials application.

The Contractor will be required to support the State in the design/build/test PeopleSoft work needed for the integration of PeopleSoft with the proposed imaging solution. In addition, the Contractor will be responsible for the Project Management of the proposed solution inclusive of all integration, testing, reporting and production implementation tasks that are specific to the Offeror proposed solution.

The Imaging solution will include a variety of types of business documents including but not limited to invoices, purchase orders, package slips, GL backup documentation, intra-agency transaction documentation, vendor documentation, and receipts for Travel and Expense.

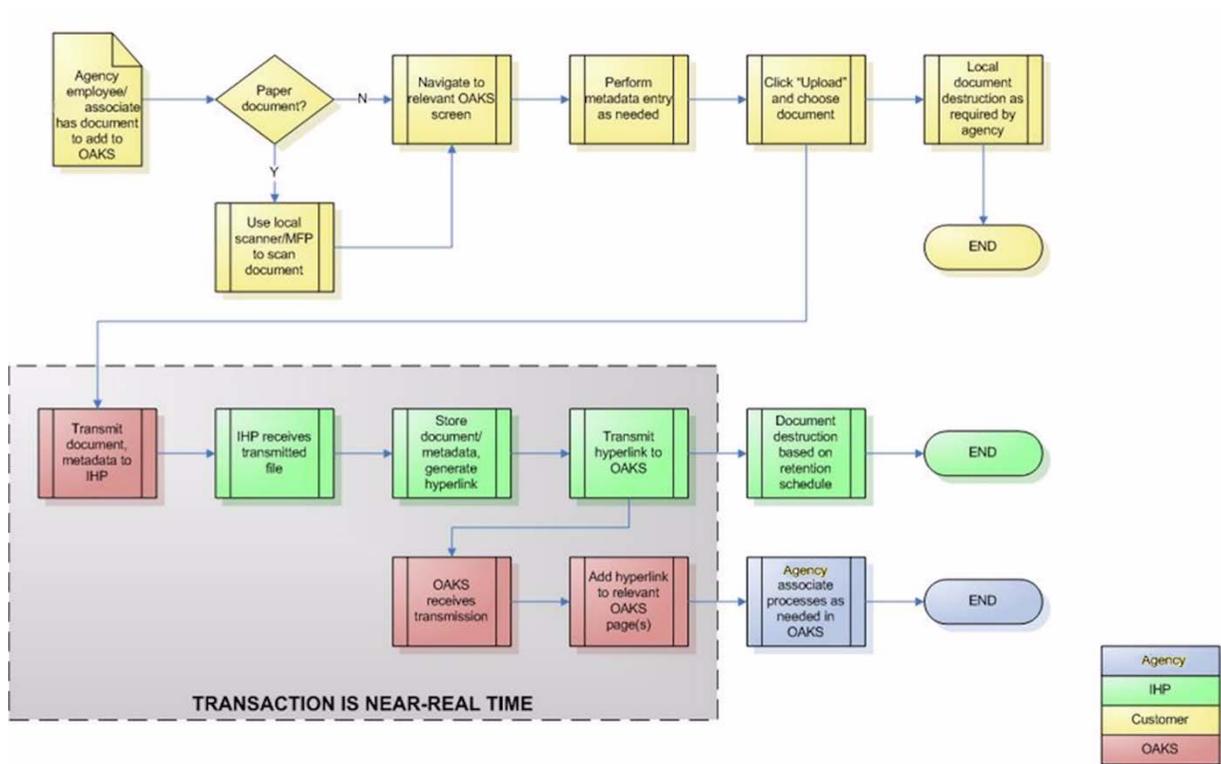
3.2. Integration Requirements

There may be a number of methods used to integrate PeopleSoft and the Offeror solution as presented in the table below. The term “Imaging Service Bureau” is used below to indicate a 3rd Party or State Internal High Volume/Capacity” Image Scanning Service outside of the scope of this Supplement.

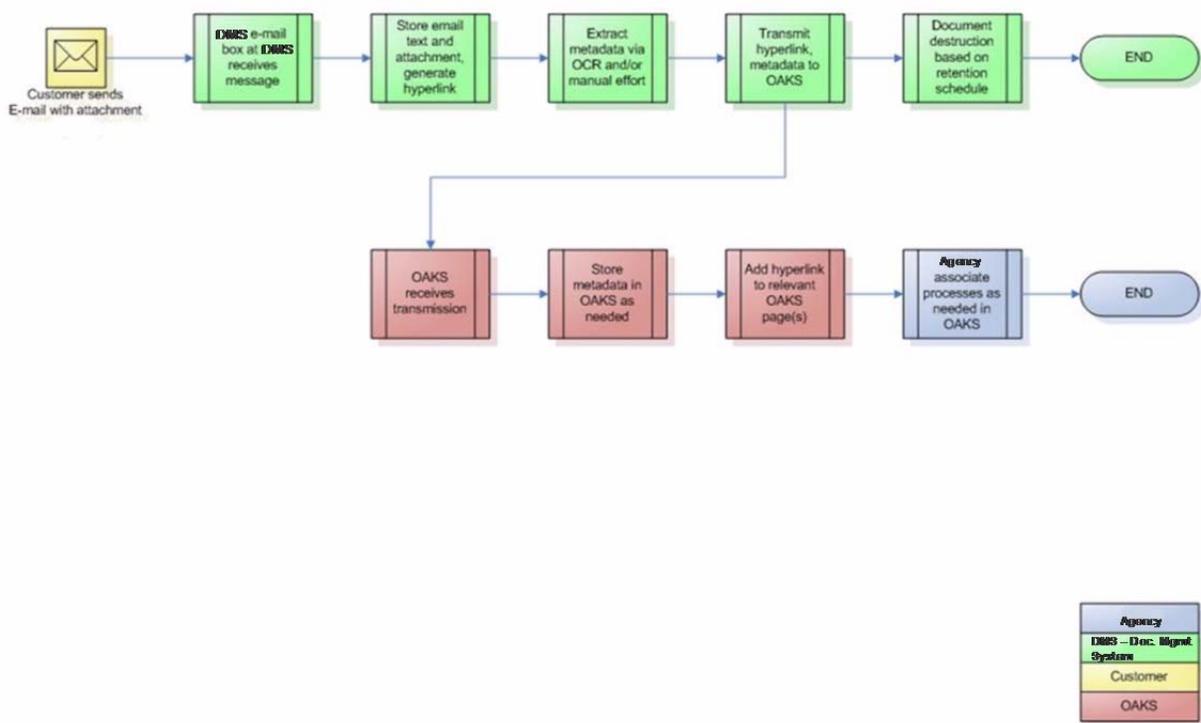
No.	Option Description	PeopleSoft Transaction	Integration Required	Outcome
1	Upload supporting documentations into PeopleSoft. No metadata associated with image	Existing transaction (Journal)	The attachment feature in PeopleTools will need to be modified or a custom attach feature will need to be built to allows users to upload documents which will they be saved at the Imaging Service Bureau.	Image will be linked to transaction. No data capture from image.
2	Send coversheet with unique fields to Offeror Imaging Service Bureau Mail copy of document to Imaging Service Bureau for scanning (document too big to scan internally)	Existing transaction	A coversheet with relevant information will need to be produced from PeopleSoft. Then, PeopleSoft will need to receive data back from the provider to associate the PeopleSoft transaction with the unique identifier for the image.	Link to image with metadata will be provided by Imaging Service Bureau and image will be linked to transaction
3	Send document and coversheet with unique fields via fax to Imaging Service Bureau	Existing transaction (e.g. Time Sensitive Documents)	A coversheet with relevant information will need to be produced from PeopleSoft. Then, PeopleSoft will need to receive data back from the provider to associate the PeopleSoft transaction with the unique identifier for the image.	Link to image with metadata will be provided by Imaging Service Bureau and image will be linked to transaction
4	Send document via mail to Imaging Service Bureau or OSSC	No existing transaction (e.g. Invoices)	PeopleSoft will need to be able to receive data from the Imaging Service Bureau (link to image, data captured off of the image) and then use it to reduce the human effort required to enter data into PeopleSoft to produce the transaction. A link will be needed to be added to relevant panels to associate the link with the transaction.	Imaging Service Bureau will return link to image, metadata and upon creation in PS, transaction (e.g. Invoice) will be linked to image
5	Send document via fax to Imaging Service Bureau	No existing transaction (e.g. Time Sensitive Invoices)	PeopleSoft will need to be able to receive data from the Imaging Service Bureau (link to image, data captured off of the image) and then use it to reduce the human effort required to enter data into PeopleSoft to produce the transaction. A link will be needed to be added to relevant panels to associate the link with the transaction.	Imaging Service Bureau will return link to image, metadata and upon creation in PS, transaction (e.g. Invoice) will be linked to image
6	Send document via e-mail to Imaging Service Bureau	No existing transaction	PeopleSoft will need to be able to receive data from the Imaging Service Bureau (link to image, data captured off of the image) and then use it to reduce the human effort required to enter data into PeopleSoft to produce the transaction. A link will be needed to be added to relevant panels to associate the link with the transaction.	Imaging Service Bureau will return link to image, metadata and upon creation in PS, transaction (e.g. Invoice) will be linked to image

3.3. Process Overview and Imaging Requirements

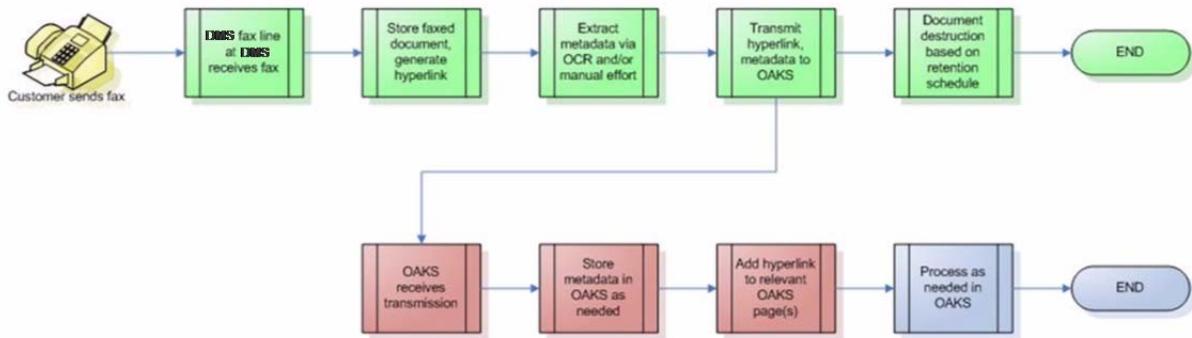
At a high level, the following imaging and PeopleSoft integration points are required by the Offeror proposed imaging solution:



3.3.3. Agency Email Upload



3.3.4. Agency Fax Upload



Supplement 3: Security and Privacy

Security and Privacy Requirements

State IT Computing Policy Requirements

State Data Handling Requirements

Contents

Supplement 3: Security and Privacy	1
Security and Privacy Requirements	1
State IT Computing Policy Requirements	1
State Data Handling Requirements.....	1
1. General State Security and Information Privacy Standards and Requirements	3
1.1. State Provided Elements: Contractor Responsibility Considerations	4
1.2. Periodic Security and Privacy Audits	5
1.3. Annual Security Plan: State and Contractor Obligations	5
1.4. State Network Access (VPN)	6
1.5. Security and Data Protection.....	6
1.6. State Information Technology Policies.....	6
2. State and Federal Data Privacy Requirements.....	7
2.1. Protection of State Data	8
2.2. Handling the State's Data.....	9
2.3. Contractor Access to State Networks Systems and Data.....	9
2.4. Portable Devices, Data Transfer and Media	10
2.5. Limited Use; Survival of Obligations.	10
2.6. Disposal of PI/SSI.	11
2.7. Remedies	11
2.8. Prohibition on Off-Shore and Unapproved Access	11
2.9. Background Check of Contractor Personnel.....	12
3. Contractor Responsibilities Related to Reporting of Concerns, Issues and Security/Privacy Issues.....	12
3.1. General.....	12
3.2. Actual or Attempted Access or Disclosure	12
3.3. Unapproved Disclosures and Intrusions: Contractor Responsibilities	12
3.4. Security Breach Reporting and Indemnification Requirements	13
4. Security Review Services.....	13
4.1. Hardware and Software Assets.....	13
4.2. Security Standards by Device and Access Type	13
4.3. Boundary Defenses.....	14
4.4. Audit Log Reviews.....	14
4.5. Application Software Security.....	14
4.6. System Administrator Access.....	14
4.7. Account Access Privileges	14
4.8. Additional Controls and Responsibilities	15

Overview and Scope

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

This scope shall specifically apply to:

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

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

1. General State Security and Information Privacy Standards and Requirements

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

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

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

State, on Contractor managed systems, supported servers and the LAN within the scope of this agreement. The Contractor will submit a draft document for State review and approval during the transition period.

The State will:

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

1.1. State Provided Elements: Contractor Responsibility Considerations

The State is responsible for Network Layer (meaning the internet Protocol suite and the open systems interconnection model of computer networking protocols and methods to process communications across the IP network) system services and functions that build upon State infrastructure environment elements, the Contractor shall not be responsible for the implementation of Security Services of these systems as these shall be retained by the State.

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

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

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

- Support intrusion detection & prevention including prompt agency notification of such events, reporting, monitoring and assessing security events.
- Provide vulnerability management services including supporting remediation for identified vulnerabilities as agreed.
- Support the State IT Security Policy which includes the development, maintenance, updates, and implementation of security procedures with the agency's review and approval, including physical access strategies and standards, ID approval procedures and a breach of security action plan.
- Support OIT in the implementation, maintenance and updating of statewide data security policies, including the State information risk policies, standards and procedures.
- Managing and administering access to the systems, networks, Operating Software or System Software, (including programs, device drivers, microcode and related code supporting documentation and media that: 1) perform tasks basic to the functioning of data processing and network connectivity; and 2) are required to operate Applications Software), systems files and the State Data.
- Supporting the State in implementation of programs to raise the awareness of End Users and staff personnel as to the existence and importance of security policy compliance.

- Installing and updating State provided or approved system security Software, assigning and resetting passwords per established procedures, providing the agency access to create user ID's, suspend and delete inactive logon IDs, research system security problems, maintain network access authority, assisting in processing the agency requested security requests, performing security audits to confirm that adequate security procedures are in place on an ongoing basis, with the agency's assistance providing incident investigation support, and providing environment and server security support and technical advice.
- Developing, implementing, and maintaining a set of automated and manual processes so that the State data access rules, as they are made known by the State, are not compromised.
- Performing physical security functions (e.g., identification badge controls, alarm responses) at the facilities under Contractor control.

1.2. Periodic Security and Privacy Audits

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

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

1.3. Annual Security Plan: State and Contractor Obligations

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

- Security policies
- Logical security controls (privacy, user access and authentication, user permissions, etc.)
- Technical security controls and security architecture (communications, hardware, data, physical access, software, operating system, encryption, etc.)
- Security processes (security assessments, risk assessments, incident response, etc.)
- Detail the technical specifics to satisfy the following:
 - Network segmentation
 - Perimeter security
 - Application security and data sensitivity classification
 - PHI and PII data elements
 - Intrusion management
 - Monitoring and reporting
 - Host hardening
 - Remote access
 - Encryption
 - State-wide active directory services for authentication
 - Interface security
 - Security test procedures
 - Managing network security devices

- Security patch management
- Detailed diagrams depicting all security-related devices and subsystems and their relationships with other systems for which they provide controls
- Secure communications over the Internet

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

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

1.4. State Network Access (VPN)

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

1.5. Security and Data Protection.

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

1.6. State Information Technology Policies

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

- Support intrusion detection & prevention including prompt agency notification of such events, reporting, monitoring and assessing security events.

- Support the State IT Security Policy which includes the development, maintenance, updates, and implementation of security procedures with the agency’s review and approval, including physical access strategies and standards, ID approval procedures and a breach of security action plan.
- Managing and administering access to the Operating Software, systems files and the State Data.
- Installing and updating State provided or approved system security Software, assigning and resetting administrative passwords per established procedures, providing the agency access to create administrative user ID’s, suspending and deleting inactive logon IDs, researching system security problems, maintaining network access authority, assist processing of the agency requested security requests, performing security audits to confirm that adequate security procedures are in place on an ongoing basis, with the agency’s assistance providing incident investigation support, and providing environment and server security support and technical advice.
- Developing, implementing, and maintaining a set of automated and manual processes so that the State data access rules are not compromised.
- Where the Contractor identifies a potential issue in maintaining an “as provided” State infrastructure element with the more stringent requirement of an agency security policy (which may be federally mandated or otherwise required by law), identifying to agencies the nature of the issue, and if possible, potential remedies for consideration by the State agency.
- The State shall be responsible for conducting periodic security and privacy audits and generally utilizes members of the OIT Chief Information Security Officer and Privacy teams, the OBM Office of Internal Audit and the Auditor of State, depending on the focus area of an audit. Should an audit issue be discovered the following resolution path shall apply:
 - If a security or privacy issue is determined to be pre-existing to this agreement, the State will have responsibility to address or resolve the issue. Dependent on the nature of the issue the State may elect to contract with the Contractor under mutually agreeable terms for those specific resolution services at that time or elect to address the issue independent of the Contractor.
 - If over the course of delivering services to the State under this Statement of Work for in-scope environments the Contractor becomes aware of an issue, or a potential issue that was not detected by security and privacy teams the Contractor is to notify the State within two (2) hours. This notification shall not minimize the more stringent Service Level Agreements pertaining to security scans and breaches contained herein, which due to the nature of an active breach shall take precedence over this notification. Dependent on the nature of the issue the State may elect to contract with the Contractor under mutually agreeable terms for those specific resolution services at that time or elect to address the issue independent of the Contractor.
 - For in-scope environments and services, all new systems implemented or deployed by the Contractor shall comply with State security and privacy policies.

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

State of Ohio Security and Privacy Policies

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

2. State and Federal Data Privacy Requirements

Because the privacy of individuals’ personally identifiable information (PII) and State Sensitive Information, generally information that is not subject to disclosures under Ohio Public Records law, (SSI) is a key element to maintaining the public’s trust in working with the State, all systems and services shall be designed and shall function according to the following fair information practices principles. To the extent that personally identifiable

information in the system is “protected health information” under the HIPAA Privacy Rule, these principles shall be implemented in alignment with the HIPAA Privacy Rule. To the extent that there is PII in the system that is not “protected health information” under HIPAA, these principles shall still be implemented and, when applicable, aligned to other law or regulation.

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

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

2.1. Protection of State Data

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

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

2.1.1. Disclosure

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

- Required by applicable law, regulation, court order or subpoena; provided that, if the Contractor or any of its representatives are ordered or requested to disclose any information provided by the State, whether PI/SSI or otherwise, pursuant to court or administrative order, subpoena, summons, or other legal process, Contractor will promptly notify the State (unless prohibited from doing so by law, rule, regulation or court order) in order

that the State may have the opportunity to seek a protective order or take other appropriate action. Contractor will also cooperate in the State's efforts to obtain a protective order or other reasonable assurance that confidential treatment will be accorded the information provided by the State. If, in the absence of a protective order, Contractor is compelled as a matter of law to disclose the information provided by the State, Contractor may disclose to the party compelling disclosure only the part of such information as is required by law to be disclosed (in which case, prior to such disclosure, Contractor will advise and consult with the State and its counsel as to such disclosure and the nature of wording of such disclosure) and Contractor will use commercially reasonable efforts to obtain confidential treatment therefore;

- To State auditors or regulators;
- To service providers and agents of either party as permitted by law, provided that such service providers and agents are subject to binding confidentiality obligations; or
- To the professional advisors of either party, provided that such advisors are obligated to maintain the confidentiality of the information they receive.

2.2. Handling the State's Data

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

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

2.3. Contractor Access to State Networks Systems and Data

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

To do this, the Contractor must:

- Use assets and techniques such as properly configured firewalls, a demilitarized zone for handling public traffic, host-to-host management, Internet protocol specification for source and destination, strong authentication, encryption, packet filtering, activity logging, and implementation of system security fixes and patches as they become available.
- Use two-factor authentication to limit access to systems that contain particularly sensitive State Data, such as personally identifiable data.
- Assume all State Data and information is both confidential and critical for State operations, and the Contractor's security policies, plans, and procedure for the handling, storage, backup, access, and, if appropriate, destruction of that data must be commensurate to this level of sensitivity unless the State instructs the Contractor otherwise in writing.

- Employ appropriate intrusion and attack prevention and detection capabilities. Those capabilities must track unauthorized access and attempts to access the State's Data, as well as attacks on the Contractor's infrastructure associated with the State's data. Further, the Contractor must monitor and appropriately address information from its system tools used to prevent and detect unauthorized access to and attacks on the infrastructure associated with the State's Data.
- Use appropriate measures to ensure that State Data is secure before transferring control of any systems or media on which State Data is stored. The method of securing the State Data must be appropriate to the situation and may include erasure, destruction, or encryption of the State Data before transfer of control. The transfer of any such system or media must be reasonably necessary for the performance of the Contractor's obligations under this Contract.
- Have a business continuity plan in place that the Contractor tests and updates at least annually. The plan must address procedures for response to emergencies and other business interruptions. Part of the plan must address backing up and storing data at a location sufficiently remote from the facilities at which the Contractor maintains the State's Data in case of loss of that data at the primary site. The plan also must address the rapid restoration, relocation, or replacement of resources associated with the State's Data in the case of a disaster or other business interruption. The Contractor's business continuity plan must address short- and long-term restoration, relocation, or replacement of resources that will ensure the smooth continuation of operations related to the State's Data. Such resources may include, among others, communications, supplies, transportation, space, power and environmental controls, documentation, people, data, software, and hardware. The Contractor also must provide for reviewing, testing, and adjusting the plan on an annual basis.
- Not allow the State's Data to be loaded onto portable computing devices or portable storage components or media unless necessary to perform its obligations under this Contract properly. Even then, the Contractor may permit such only if adequate security measures are in place to ensure the integrity and security of the State Data. Those measures must include a policy on physical security for such devices to minimize the risks of theft and unauthorized access that includes a prohibition against viewing sensitive or confidential data in public or common areas.
- Ensure that portable computing devices must have anti-virus software, personal firewalls, and system password protection. In addition, the State's Data must be encrypted when stored on any portable computing or storage device or media or when transmitted from them across any data network.
- Maintain an accurate inventory of all such devices and the individuals to whom they are assigned.

2.4. Portable Devices, Data Transfer and Media

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

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

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

2.5. Limited Use; Survival of Obligations.

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

2.6. Disposal of PI/SSI.

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

2.7. Remedies

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

2.8. Prohibition on Off-Shore and Unapproved Access

The Contractor shall comply in all respects with U.S. statutes, regulations, and administrative requirements regarding its relationships with non-U.S. governmental and quasi-governmental entities including, but not limited to the export control regulations of the International Traffic in Arms Regulations ("ITAR") and the Export Administration Act ("EAA"); the anti-boycott and embargo regulations and guidelines issued under the EAA, and the regulations of the U.S. Department of the Treasury, Office of Foreign Assets Control, HIPPA Privacy Rules and other conventions as described and required in this Supplement.

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

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

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

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

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

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

2.9. Background Check of Contractor Personnel

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

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

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

3. Contractor Responsibilities Related to Reporting of Concerns, Issues and Security/Privacy Issues

3.1. General

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

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

3.2. Actual or Attempted Access or Disclosure

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

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

3.3. Unapproved Disclosures and Intrusions: Contractor Responsibilities

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

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

3.4. Security Breach Reporting and Indemnification Requirements

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

4. Security Review Services

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

4.1. Hardware and Software Assets

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

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

4.2. Security Standards by Device and Access Type

The Contractor will:

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

4.3. Boundary Defenses

The Contractor will:

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

4.4. Audit Log Reviews

The Contractor will:

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

4.5. Application Software Security

The Contractor will:

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

4.6. System Administrator Access

The Contractor will

- Inventory all administrative passwords (application, database and operating system level)
- Implement policies to change default passwords in accordance with State policies, particular following any transfer or termination of personnel (State, existing MSV or Contractor)
- Configure administrative accounts to require regular password changes
- Ensure service level accounts have cryptographically strong passwords
- Store passwords in a hashed or encrypted format
- Ensure administrative accounts are used only for administrative activities
- Implement focused auditing of administrative privileged functions
- Configure systems to log entry and alert when administrative accounts are modified
- Segregate administrator accounts based on defined roles

4.7. Account Access Privileges

The Contractor will:

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

4.8. Additional Controls and Responsibilities

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

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

SUPPLEMENTAL INFORMATION TRAILER

This page is the last page of supplemental information for this competitive document. If you received this trailer page, all supplemental information has been received.

Note: portions of the supplemental information provided may or may not contain page numbers. The total number of pages indicated on the cover page does not include the pages contained in this supplement.