ATTACHMENT I: SCOPE OF SERVICES

I. Optional Infrastructure Support Transition to SSRC

In the event that the Department elects to end or terminate Optional Infrastructure Support Services, as outlined in VII. Scope of Work and VIII. Transition and Termination Services (Section A.3), the following two sections will replace in their entirety Attachment I: Section B.1 Requirements and Section B.3. Infrastructure/Technical Support Responsibilities Matrix.

I.1 Requirements

Accenture acknowledges and accepts all Application Management requirements as outlined below.

Requirement	How Accenture will Meet this Requirement
Apps-001: Provide support and maintenance for the Ariba Suite (Buyer, Analysis, and Sourcing) and its customizations, interfaces, batch jobs, and reports, ensuring adequate performance and accurate processing. Includes applying application patches (for security and bug fixes) in a timely manner and implementing enhancements to the current version as they become available. (The Ariba application went through a major upgrade to Buyer 9r1 in the third quarter of 2011, along with hardware upgrades. A major upgrade is not planned in the new Contract.)	• The Application Management team will provide functional testing and performance testing/tuning needed to support the customized Ariba applications and related batch jobs and reports. • We will evaluate Ariba application patches and coordinate and schedule any planned implementations with DMS. • We will use our ADM methodology and PMI principles to guide our team in support and maintenance activities
Apps-002: Provide support and maintenance for the VIP applications. Support of this application may be removed from this contract after the first year and moved to internal State resources.	• The Application Management team designed and developed the Java SpringSource-based Vendor Information Portal (VIP) application. The VIP includes the Billing and Collections, Vendor Registration, and Vendor Performance Tracking applications. It also contains the Spring-batch components to manage many of the complex file-based batch interfaces used by the MFMP System. As the creator of this application, our team will leverage its knowledge of VIP to provide quality ongoing support and knowledge transfer to the State, if requested. • The Application Management team will provide functional testing and performance testing/tuning needed to support the custom VIP applications and related batch jobs and reports. • We will use our ADM methodology and PMI principles to guide the team in its support and maintenance activities.

Requirement	How Accenture will Meet this Requirement
Apps-003: The Service Provider will maintain a development environment at their physical site, to include the necessary software tools and hardware, to support, maintain, and enhance the Ariba suite, the VIP applications, and any other systems used in the operations of the MFMP Program, the monitoring of system health and availability, and the monitoring of system transactions to verify successful completion of these transactions.	• The Application Management team will maintain individual virtual environments for each developer. • We will use industry standard application development tools such as, but not limited to, Eclipse Java IDE, TOAD, Araxis, Perforce, and Artifactory. • We will handle application code and repository versioning tools, such as Perforce. Code versioning will help the team maintain an audit trail detailing developer-specific updates for application code which creates a tight quality control within the development environment. • We will use the development, system testing, and performance testing environments to support application management activities. This will enable coding changes to be implemented in a controlled environment where they are carefully tested for confirmation of intended functionality and we validate that the changes do not negatively impact online response time or existing functionality. • We will use custom FLAIR integration monitoring. • We will use a monitoring tool, such as HP Business Availability Center (BAC), to monitor system performance from a user experience within the specified MFMP Systems to measure how long it takes for a screen to return after a user clicks a button. • We will use monitoring tools, such as SiteScope and BAC, to provide alerts of potential outages of the MFMP applications. These alerts will be sent automatically to our 24-hour on call resources. • We will use processes and tools tailored to monitor the MFMP System.
Apps-004: Monitor performance of all applications to ensure a positive user experience by all users of the MFMP applications.	• The Application Management team will use a monitoring tool, such as HP Business Availability Center (BAC), to monitor system performance and availability from a user experience within each MFMP System.

Apps-005: Monitor all production batch jobs and system processes, ensuring successful completion and accurate processing.	• Using industry standard tools, Accenture has developed specifically for MFMP an extendible batch framework to monitor production batch jobs. The tools used include a custom MFMP-specific master batch shell-based program that provides daily status of the batch jobs that run each night.
	• We will use a proven, custom Java SpringSource batch management program to organize, monitor, and if needed recover failed batch jobs.
	• We will review the Daily Master Batch results each morning. Those results summarized will include:
	  – Manually verified status of all MFMP production applications
	  – Punch-out verification

Requirement	How Accenture will Meet this Requirement
	– Training environments verification – Confirmation that the iWay integration component used to send and receive messages with FLAIR is fully operational – Summary of major data loads and their processing times (Analysis load, OSD load, FLAIR Chart of Accounting load, VIP vendor load to Buyer) – System defects (identified as SIRs) that are being monitored for additional research or for production workaround • We will coordinate batch recovery as necessary. •
Apps-006: Monitor all production report generation, ensuring successful completion and accurate report results.	• The Application Management team will use a custom reporting solution to generate agency requested ad-hoc reports. • We will configure the automated monitoring to: – Alert the Application Management team of report creation issues. – Verify that reports are created and posted. For any report issues our application management team will work to correct and post as soon as possible.
Apps-007: Monitor the FLAIR interface and related system logs to ensure successful transactions and accurate information, working closely with DFS on any and all issues.	• We will use multiple tools and processes, such as SiteScope, CA Wily Introscope, and custom iWay integration monitoring scripts, to monitor the health of the MFMP-FLAIR real-time interface. • We will perform production support activities daily to monitor failed transactions. • We will also oversee an automated queued transaction recovery task that will run at regular intervals during business hours to coincide with FLAIR uptime. • When a FLAIR issue occurs, we will work together effectively with DFS to resolve any issues between the two systems quickly and with minimal impact to the users.
Apps-008: Maintain up-to-date, adequate system documentation, documenting applications specifics, architecture information, and configuration.	• The Application Management team will maintain necessary application and technical documentation related to the MFMP Systems. • We will manage the documentation carefully for version control. The documentation is available for troubleshooting and for guiding consistent maintenance and monitoring of applications. The documentation will be available to MFMP team members and to DMS leadership. It will be stored on the project Sharepoint for easy accessibility. The documentation includes: – Operation plans – Configuration management plans – Disaster recovery plans – Code migration processes – Batch schedule – iWay component configuration

Requirement	How Accenture will Meet this Requirement
	– Interface and integration manuals – Technology Plan – Existing design documents – Code repository processes
Apps-009: Maintain a positive relationship with the SSRC and work collaboratively with the SSRC to ensure proper performance and availability of all MFMP Program systems.	• The Accenture team relocated the MFMP infrastructure to the SSRC in 2007 and is familiar with the SSRC processes and people. • We will maintain a positive and collaborative working relationship with the SSRC. • To facilitate the most effective working relationship, the MFMP Application Management team will meet with SSRC representatives regularly, with a goal of at least monthly meetings. We will also be proactive in discussing significant upcoming infrastructure and application changes that require SSRC participation or may impact their ability to fulfill their responsibilities as it relates to MFMP support. We will also be responsive in cooperating with SSRC personnel regarding upcoming changes to SSRC infrastructure that may impact the MFMP environment. • We have worked with the SSRC and DMS to align our responsibilities, as defined in the Responsibilities Matrix in section 2.3 below.
Apps-010: Maintain a Disaster Recovery plan, in coordination with the SSRC, that outlines steps to fail over production processing for Ariba Buyer to the DR site, and steps to recover from a disaster and move processing successfully back to the SSRC. DMS requires a Recovery Time Objective (RTO) of 24 hours, and a Recovery Point Objective (RPO) of one hour. The disaster recovery plan should reflect these objectives. The service provider is expected to support the disaster recovery plan with application management and support service.	• The Application Management team will follow an MFMP disaster recovery (DR) plan. • We will test the MFMP disaster recovery site annually in collaboration with SSRC and update the plan as necessary. • In order to achieve the RTP and RPO specified, the SSRC must license Oracle DataGuard for implementation to support disaster recovery. This purchase would be included with the Oracle database license purchase and maintenance which is the responsibility of the Department unless the option for Service Provider to make these purchases is elected.
Apps-011: Evaluate the Disaster recovery plan and make recommendations to include the VIP.	• We will perform an evaluation of the current DR infrastructure and licensing to establish an estimate and a plan for implementing DR for VIP.
Apps-012: Test the Disaster Recovery plan once per year, and deliver the results to the DMS Chief Information Officer.	• We will test the MFMP disaster recovery site annually in collaboration with SSRC. • We will deliver and review the results of the test with the DMS Chief Information Officer and other DMS project management team members.

Requirement	How Accenture will Meet this Requirement
Apps-013: Provide maintenance and support for all applications used internally (within the MFMP Program) to automate and support MFMP operations, which might include IVR system, help desk software, ticket tracking system, system monitoring applications, training development applications, bug tracking applications, etc.	• Our team will perform regular maintenance activities on the applications needed to support internal operations of the MFMP Program. Major internal applications include: help desk tools, MFMP active directory, ticket tracking, code repository, development IDE tools, performance monitoring tools, system monitoring tools, MFMP IVR and call routing, MFMP development tools, MFMP development/test environment, and MFMP project site domain/tools backup management. • We will use email services from the State for project based email accounts for communications with customers of the system. This will require that the State provide a total of approximately 25 email accounts for the MFMP team members and listserv capabilities.
Apps-014: Perform Tier 3 support for help desk and trouble tickets involving data issues or application processing.	• The Application Management team will work collaboratively with the Help Desk team on ticket escalations. • We will escalate tickets not resolved at the Tier 2 level to Tier 3, and resolve tickets at the Tier 3 level in accordance to the SLE defined timeframe.
Apps-015: Assist with research and problem resolution to finance and accounting discrepancies between Ariba information and the state's FLAIR system.	• We will monitor and evaluate the reconciliation of FLAIR transactions with the MFMP Buyer applications. • We will provide the Department of Financial Services (DFS) a file with MFMP payment information from the previous month by the 20th of each month. MFMP will receive reconciliation files from DFS by the 25th of each month. Our team will then analyze the reconciliation data. • We will conduct monthly meetings with the DMS team to review the number of process transactions and error rate (those transactions that were not reconciled). • We will record system issues and distribute the information for research. • We will work with the DMS team to notify agencies of un-reconciled transactions that are not a result of system issues (such as mismatches on disbursement transactions that were marked as paid directly in FLAIR).
Apps-016: Assist with catalog additions, changes, and deletions as necessary.	• We will deliver high quality and timely catalog additions, updates, and deletions.
Apps-017: Assist with incorporating any documents or data into the Ariba and VIP applications that may require developer or technical assistance.	• The Application Management team will support the Department's needs to implement changes (several examples include modifications related to units of measure, methods of procurement, commodity codes, news feeds, terms of use and business rules) utilizing standardized processes. • We will assist the Department in evaluating system impacts as a result of Florida statute or rule changes. • For changes requiring customization to the Ariba or VIP applications, we will provide estimated level of effort, and

Requirement	How Accenture will Meet this Requirement
	changes may be implemented at the Department's discretion using Service Hours.

Apps-018: Load data feeds from external sources like FLAIR into the Analysis module for reporting and analytics	• The Application Management team will monitor, manage, and support the loading of data into the Ariba application including, but not limited to, the two existing FLAIR data loads:
	  – Weekly encumbrance information
	  – Monthly payment information
	
	• For any new external sources of data to be loaded into the Analysis module, we will provide estimated level of effort, and changes may be implemented at the Department's discretion using Service Hours.

Apps-019: Ensure fulfillment of production and ad-hoc report requests.	• The Application Management team will support agency ad-hoc monthly report requests in accordance to the related service level expectation (SLE). • We will use the Department's FTP reporting website and Analysis reports to meet agencies' reporting needs.
Apps-020: Respond to minor customization requests for VIP and Ariba due to rule changes, statute changes, FLAIR changes, or enterprise processing changes.	• The Application Management team will work with the Department's project team to estimate, design, develop, test, and implement customizations. • Any such customization requests requiring less than 40 hours to implement will be done as a standard part of Application Management services. For any change requiring 40 or more hours to implement, we will provide the estimated level of effort, and changes may be implemented at the Department's discretion using Service Hours.
Apps-021: Directly interface and work closely with any other vendor contracted to interface with or make changes directly to the Ariba suite or VIP application. DMS reserves the right to contract with a different vendor for more substantial system changes that require additional costs, if it is in the best interest of the state.	• The Application Management team will collaborate with vendors contracted by the Department for enhancing the MFMP Program. We will work closely and collaboratively with Ariba, the SSRC and DMS IT, in addition to the vendor(s).
Apps-022: Comply with Florida Information Technology Resource Security Policies and Standards (Chapter 71A-1, Florida Administrative Code.)	• The Application Management team will operate and maintain the MFMP suite of applications in accordance to the Florida Information Technology Resource Security Polices and Standards (Chapter 71A-1, FL Administrative Code).
Apps-023: Comply with s. 508 of the Rehabilitation Act of 1973, as amended and 29 U.S.C. s. 794(d), including the regulations set forth under 36 C.F.R. part 1194. Section 282.601(1), F.S., states that "state government shall, when developing, competitively procuring, maintaining, or using electronic information or information technology acquired on or after July	• The Application Management team will work with agencies and customers that require special assistance in accessing the Ariba or VIP applications. • We will work with agencies in a manner consistent with what we have done in the past. For example, for the Florida School of Deaf and Blind Services agency customers, we provided one-on-one support and coaching.

Requirement	How Accenture will Meet this Requirement
1, 2006, ensure that State employees with disabilities have access to and are provided with information and data comparable to the access and use by State employees who are not individuals with disabilities."	
Apps-024: Establish a system fix/change review process with the Department for reviewing and prioritizing system development efforts.	• The Application Management team will conduct regularly scheduled bi-weekly meetings of the SIR Review Board (SRB) to review all open system investigation requests (SIRs). The SRB consists of Department MFMP Program members and Accenture project team members. • During the review meetings we will work together to categorize and prioritize new SIRs, and confirm closure of implemented SIRs. • We will schedule upcoming system changes, including SIRs, change requests, infrastructure maintenance and system patches.
Apps-025: Prepare design documentation and estimates for change requests submitted by the Department. The Service Provider will be responsible for tracking all change requests.	• The Application Management team will provide estimates and design documentation for change requests approved by the Department. • We will review those change request documents with Department's MFMP project leadership as well as agency representatives assigned to the change review board (CRB).
Apps-026: A root cause analysis report shall be provided to the Department within three business days of any system outage.	• The Application Management team will develop root cause analysis (RCA) documents within three business days of any MFMP System outage. • The RCA will include a timeline of events, description of problem, lessons learned, SSRC impacts and dependencies, and corrective actions applied to mitigate future outages. • The RCA will also include any 3rd party support ticket information (MyFloridaNet, Oracle, Ariba, Cisco, F5, IBI, DFS FLAIR support, etc.) that is relevant to the MFMP System outage.
Apps-027: The contract SLEs will apply to the performance of Buyer running under an activated disaster recovery, and will require similar application monitoring. The Service Provider will be held to the SLEs within their responsibility.	• In the development of the Disaster Recovery Plan, consideration will be taken to enable the application SLEs to be met in a failover scenario to the disaster recovery site.
Apps-028: The Service Provider initiates the MFMP Payment reconciliation process with DFS. By the 20th of each month the Service Provider will send DFS a payment record file containing the prior month's transactions. DFS will provide an updated file within 5 business days. The Service Provider shall reconcile the payments as indicated in SLE-022 by the 15th of the month following the receipt of the file.	• Accenture will prepare the payment reconciliation file monthly to include payments in MFMP from the prior month. This file will be provided to DFS who will then return the file updated with payment reconciliation information from FLAIR. Accenture will then complete reconciliation as needed with the files and summarize the results by the 15th of the following month. • Results will be reviewed with DMS as requested.

Requirement	How Accenture will Meet this Requirement
	• Accenture will maintain comprehensive testing documentation, including detailed procedures and testing scripts, which are updated on a regular basis for system enhancements and when new issues are identified
	• Accenture will coordinate with State Term Contract vendors to support testing and implementation of electronic interfaces through the Ariba Network, including punch-out catalogs, purchase order issuance, and electronic invoice processing
	• We will periodically refresh the Buyer training database with production-like data to make the training exercises for agency users more realistic and useful
	• We will support and collaborate with DIS team within DFS to support MFMP interface testing with their infrastructure and code changes, such as supporting their software upgrades (CICS Natural, etc.) and FLAIR disaster recovery testing
	• Accenture will support Department communications by coordinating the inclusion of State Purchasing messaging within the MFMP applications
	• We will deploy scripts, such as HP BAC agents, to agency locations as needed to help troubleshoot anomalies in online response time in a particular building
	• Accenture will install and configure tools, such as Wily Introscope, to monitor specific components of application performance, providing the Application Management team with additional troubleshooting support, but also providing insight to Department personnel regarding the overall health of the application at any point in time
	• We will incorporate extensive quality assurance practices in system development and configuration management, including complete system quality checks after every code release which prevents interruptions to business processing
	• We will perform an evaluation of the current MFMP reporting capabilities within Contract Year 1 in collaboration with the Department. The evaluation will consider the State's two high level reporting needs: 1) analytical reporting to understand/evaluate spending patterns in support of strategic sourcing and effective management of the State's spending/contracting practices going forward; and 2) operational reporting in support of day-to-day, week-to-week and month-to-month purchasing and F&A agency transaction management, including reviews of procedural patterns by any reviewing entity such as the auditors. The evaluation will result in a recommendation for continuation, modification and/or replacement of existing MFMP reporting capabilities including Ariba Analysis and the FTP Reporting Site. Any changes that are to be implemented from this evaluation would need to be covered through Service Hours or through a

Requirement	How Accenture will Meet this Requirement
	change order with separate payment.

I.3 Infrastructure/Technical Support Responsibilities Matrix

The technical and infrastructure management primary responsibilities for the MFMP systems between Accenture and the Southwood Shared Resource Center (SSRC) are defined as outlined below.

Task	Responsible		Comments
	Accenture	**SSRC**	
Operations			
Tape Backup		✔	
Hardware Maintenance & Upgrades		✔	Accenture team will inform SSRC of hardware upgrades needed based on application and business requirements
System Monitoring		✔	SSRC provides uptime monitoring 24x7
Security Monitoring		✔	SSRC handles intrusion detection at all layers, except the network, which is handled by DivTel
Application Security Testing	✔		
Storage Management		✔	
License Renewals for Operating System and Database Software		✔	
Database Administration			
Access Control & Audit	✔		SSRC will grant Accenture access to view log files containing system access and modifications
Session Monitoring	✔		If Accenture cannot see and terminate sessions for any reason a ticket will be opened with SSRC and responsibility will transfer at that time to the SSRC
User Creation & Administration	✔		
Space Management & Allocation		✔	ASM, NFS Mounts, etc.
Oracle Memory Administration & Monitoring		✔	Accenture will have the ability to monitor in addition to SSRC
Oracle Memory Tuning & Recommendations		✔	Accenture will provide recommendations to SSRC and receive alerts
Creation & Analysis of Oracle AWR Reports	✔		
Schema & Table Creation	✔		
Database Instance Backup & Restore		✔	Accenture can import and export tables
Script & Cron Management at User Account Level	✔		Jobs which do not require Oracle/Root User Account to run
Script & Cron Management at Oracle/Root User Account Level		✔	Jobs which require Oracle/Root User Account to run
Database Patch Compatibility Research for Infrastructure		✔	SSRC will validate that patches are compatible with other infrastructure components
Database Patch Compatibility Research for Applications	✔		Accenture will validate that patches are compatible with applications

Task	Responsible		Comments
Patch Implementation for Hardware & OS		✔	
Application Patch Implementation	✔		
SQL Development	✔		
Systems Administration			
Application Code Deployment (Ariba, SpringSource, iWay)	✔		
Application Interface Management & Recovery	✔		
Network Interface Management & Recovery		✔	
Operating System, Hardware, Storage Patch Compatibility Research for Infrastructure		✔	SSRC to confirm patches are compatible with other infrastructure components
Operating System, Hardware, Storage Patch Compatibility Research for Applications	✔		Accenture to confirm patches are compatible with applications
Patch Implementation		✔	
Ariba Application Configuration	✔		
Application Monitoring (Ariba, SpringSource, iWay)	✔		
Storage Monitoring		✔	
Storage Capacity Planning	✔		
Environment Build Out through DB Layer		✔	
Environment Build Out for Application & Web Layers	✔		
Disaster Recovery Testing	✔	✔	
Operational Data Updates	✔		
Project Site Development & Infrastructure Management	✔		
Ariba Email Configuration & Administration	✔		
Network Administration			
Project Site Management & Administration	✔		
Application Load Balancing (F5s)		✔	
Certificate Management	✔		
MFMP System Firewall at SSRC		✔	Accenture will provide rules
MFMP Cisco ASA		✔	
MFMP System Firewall at		✔	Accenture will provide rules

Task	Responsible		Comments
QTS			
QTS Cisco ASA		✔	
Security Scans & Remediation		✔	
Secure Tunnel Management for SSRC & QTS		✔	SSRC has primary responsibility for these connection points, but if connection terminates at project site that point is owned by Accenture
Secure Tunnel Management for Project Site	✔		Accenture is responsible for connection at Project Site
Cisco Switch Management		✔	
Performance Management			
Capacity Planning	✔		
Hardware & Infrastructure		✔	
System Diagnostics	✔		
Application Performance Monitoring	✔		
Ariba Analysis & Tuning	✔		
JVM Analysis & Tuning	✔		
BEA Weblogic Analysis & Tuning	✔		
iWay Interface Analysis & Tuning	✔		
Apache Analysis & Tuning	✔		
Oracle Analysis & Tuning	✔		
Project Site Network Analysis & Tuning	✔		
SSRC & QTS Network Analysis & Tuning		✔	
Load Testing	✔		
Agency Performance Triage & Research	✔		