

**Appendix 14 to
Second Amendment of
Master Service Agreement**

June 25, 2012



**Exhibit to Data Center Services
Service Component Provider
Master Services Agreement**

DIR Contract No. DIR-DCS-SCP-MSA-002

Between

**The State of Texas, acting by and through
the Texas Department of Information Resources**

and

Xerox State & Local Solutions, Inc.

**Exhibit 19
Transition Plan**

June 25, 2012

TABLE OF CONTENTS

1.0	TRANSITION MANAGEMENT	3
1.1	Introduction	4
1.2	Document Overview.....	4
2.0	TRANSITION GUIDING PRINCIPLES	4
3.0	TRANSITION OBJECTIVES	5
4.0	TRANSITION APPROACH AND PROJECT METHODOLOGY	6
5.0	TRANSITION OVERVIEW.....	8
5.1	Transition Staffing	9
5.2	Transition Coordination and Integration.....	9
5.2.1	Cross-Functional Services Transition	9
5.3	Transition by Service Component.....	16
5.3.1	Mainframe Service Component Transition.....	16
5.3.2	Server Service Component Transition	18
5.3.3	Data Center Service Component Transition	21
5.3.4	Network Service Component Transition.....	22
6.0	SERVICE PROVIDER TRANSITION ROLES AND GOVERNANCE ALIGNMENT	24
7.0	QUALITY CONTROL AND GENERAL RISK MITIGATION.....	25
8.0	COMMUNICATIONS.....	26

EXHIBIT 19
TRANSITION PLAN

Update Methodologies and Attachments to Exhibit 19

The following update methodologies and attachments are incorporated as part of **Exhibit 19**:

Title	Methodology for Updating Associated Exhibit Attachments
<u>Exhibit 19</u> Transition Plan	<u>Exhibit 19</u> is updated in accordance with <u>Section 4.2(b)</u> of the MSA.
<u>Attachment 19-A</u> Transition Milestones	<u>Attachment 19-A</u> shall be updated in accordance with <u>Section 4.2(b)</u> of the MSA.

1. TRANSITION MANAGEMENT

1.1 Introduction

In accordance with Section 4.2 of the Agreement, this Exhibit 19 and the attached Attachment 19-A collectively constitute the Transition Plan, and references to the Transition Plan in this Agreement (including this Exhibit) shall be read and understood to collectively mean this Exhibit 19 and the attached Attachment 19-A. Service Provider shall maintain and implement the Transition Plan, and any modifications to the Transition Plan shall be subject to DIR's review and approval in accordance with Section 4.2 of the Agreement.

The provisions of the Transition Plan are in addition to, and not in lieu of, the terms and conditions contained in the body of the Agreement and the other Exhibits and Attachments thereto; provided however, unless otherwise expressly stated, the provisions of this Transition Plan shall not control over conflicting provisions of the Agreement. Unless otherwise expressly defined in the Transition Plan, capitalized terms used in the Transition Plan shall have the meaning assigned to them elsewhere in the Agreement.

The dates in this document are intended to provide context and set expectations for the solutions described. Actual milestone dates are contained in the appropriate milestone documents (Attachment 19-A Transition Milestones and Attachment 20-A Transformation Milestones). In the event of a conflict in dates the dates in the milestone documents will control.

1.2 Document Overview

Transition consists of those standard activities necessary for the Service Provider to assume service delivery responsibility from the State beginning on Commencement Date. These activities include the transfer of staff, establishment of the IT environment, setup of the program management system, implementing workplace logistics, and deploying any necessary interim processes and tools.

2. TRANSITION GUIDING PRINCIPLES

The Service Provider will:

Provide a customized approach to meet the needs of DIR which includes:

- ♦ DIR and DIR Customer transition models
- ♦ Experienced transition project managers
- ♦ Leveraging Service Provider's tools and templates customized to the DIR and DIR Customer environments

Establish strong governance, which includes:

- ◆ Clearly defined roles and responsibilities
- ◆ Jointly developed processes
- ◆ Effective meetings and reporting framework to minimize resource requirements while achieving goals
- ◆ Mechanisms in place to identify and address risks and issues early
- ◆ Support for OLA development

Maintain effective communication, which includes:

- ◆ Consistent delivery of key messages through well-defined communication plans
- ◆ Tailored communications to target audiences and stakeholders
- ◆ Mutually agreed frequency of communications to meet the needs of the stakeholders

Promote collaboration and teamwork , which includes:

- ◆ Detailed upfront project planning and feedback
- ◆ Joint agreement on status for reporting purposes
- ◆ Plans scaled to address DIR Customer differences in size and complexity
- ◆ Establishment and support for successful deliverable review process
- ◆ Feedback on deliverables throughout the life of the project.

3. TRANSITION OBJECTIVES

The key objectives of Transition are:

- To take over Services from the Incumbent Service Provider within six (6) months of the Effective Date and with minimal impact on the performance of the operations.
- Ensure that the Service Provider steady state team has sufficient knowledge, documentation and resources to manage the operations at Commencement
- Implement the Service Management tools and solutions to facilitate effective Service Management at Commencement

The Service Provider will achieve these objectives by dividing the Transition into two phases (Phase I and Phase II). During Phase I, the Service Provider will focus its attention on activities that will enable the Service Provider to take over support of the environment at Commencement while ensuring no degradation of service to DIR and DIR Customers. Activities include acquiring sufficient knowledge and deploying the appropriate number of resources to ensure a seamless Transition of service from the Incumbent Service Provider to the Service Provider. Where possible, the Service Provider will improve operations documentations, including run books and Technical Recovery Guides (TRGs) and deploy its Service Management tools during Phase I to enable response to events before being alerted about the events by DIR or DIR Customers. These tools will be dormant until Commencement,

unless approved by DIR. Section 4.0 of this document provides more detail about the activities the Service Provider plans to perform during this phase.

During Phase II, the Service Provider will accomplish the activities that were not required in order to Transition services from the Incumbent Service Provider. In cases where the Service Provider was unable to install its Service Management tools during Phase I, the Service Provider will install them during Phase II. The Service Provider understands that some systems may not have the capacity to accept additional tools. In this case, the Service Provider will manage the systems as they are managed by the Incumbent Service Provider. Section 4.0 of this document provides more detail about the activities the Service Provider plans to perform during this phase.

Major Transition activities include the following:

- Staffing appropriately for Transition and Commencement support
- Performing knowledge transfer from the Incumbent Service Provider
- Performing knowledge transfer from DIR Customers for areas In-Scope for the Service Provider that the Incumbent Service Provider is not performing today
- With agreement by the Parties, deploying tools onto In-Scope systems that are not being monitored today
- Integrating with the tools and processes established by the MSI
- Minimizing the number of interactions to the DIR Customers and Incumbent Service Provider
- Completing Critical Deliverables as described in **Exhibit 3**.

4. TRANSITION APPROACH AND PROJECT METHODOLOGY

The Service Provider's Transition approach is to drive a low-risk, highly transparent program that will enable the Service Provider to meet the milestones and ensure readiness to take over Services from the Incumbent Service Provider by Commencement. The Service Provider will assign resources to Transition dedicated to planning, coordinating, executing and managing the Transition tasks.

The approach includes a one (1) year Transition consisting of two phases (Phase I and Phase II).

- **Phase I.** During the first six (6) months, the Service Provider will focus on activities related to service Commencement, including:
 - creating the on-boarding and off-boarding process with the MSI
 - developing the HR transition plan
 - developing the integrated templates with the MSI
 - preparing organizational communications plans

- onboarding staff
- working with the MSI in the integration of tools, processes and training
- performing asset inventory (physical and logical)
- acquiring software consents
- support of Resource Baseline True-Up
- conducting knowledge transfer
- deploying the necessary Service Provider management tools for Commencement day readiness

Incumbent Service Provider personnel who are hired by the Service Provider will re-badge on the Commencement Date. If the Service Provider is unable to improve documentation and install their tools onto systems during Phase I, at Commencement the Service Provider will manage the systems as they are managed by the Incumbent Service Provider and start tool installation during Phase II of Transition. For systems with no monitoring, the Service Provider will be made aware of outages when users have a problem and call into the Service Desk to initiate the Incident Management process.

- **Phase II.** Over the remaining six (6) months, the Service Provider will complete Transition to the end-state support model, including uninstalling Incumbent Service Provider tools that are replaced by the Service Provider's tools and refining processes and documentation with the MSI. For situations where the Service Provider is unable to install tools during Phase I, the Service Provider will install those tools during Phase II. The Service Provider will work closely with the MSI to reconcile the asset inventory data received from Phase I for Resource Baseline True-Up in Phase II. Outstanding software licensing, asset transfer activities, and service tools deployment also will be completed in Phase II.

Continuity Plan; conducting knowledge transfer and deploying the necessary management tools for Commencement day readiness. As a part of Phase II, the Service Provider will complete Transition to the end-state support model, including refining processes and documentation with the MSI. The Service Provider will work closely with the MSI to reconcile the asset inventory data received from Phase I for True-Up in Phase II. Outstanding software licensing, asset transfer activities, and service tools deployment also will be completed in Phase II.

5.1 Transition Staffing

To staff the Transition team, the Service Provider will use a blend of existing experienced Service Provider employees as well as hire new experienced employees. The staff assigned to work Transition will be specific to Transition and separate from the steady state team. The Service Provider plans that more than 75% of the staff from Phase I Transition will be assigned to work on the steady state team. The Service Provider will accomplish this by staffing individuals from the steady state team during Phase I to work Transition. This will ensure continuation of the knowledge from Transition. Upon Commencement, these resources will transfer to the steady state team and remain on the account with the knowledge they've acquired from the Phase I Transition. The resources who continue to work on Transition during Phase II will be separate from the steady state team.

The team will be made up of:

- Transition Managers
- HR Administrators
- Systems Engineers
- Systems Administrators
- Process Managers
- Security Engineers
- Tools Engineers
- Architects

5.2 Transition Coordination and Integration

As part of Transition, the Service Provider will work to ensure the Service Provider's processes, people and tools are coordinated and integrated with the MSI, DIR, and DIR Customers. The section below describes the Service Provider's plan for the cross-functional coordination and integration activities.

5.2.1 Cross-Functional Services Transition

As part of the Cross-Functional Services Transition, Service Provider will:

1. Establish Transition governance
2. Actively participate in the configuration and integration of the MSI's ITSM tool
3. Actively participate in training activities
4. Actively participate in the Security Program
5. Actively participate in the Disaster Recovery program
6. Provide input to the Service Management Manual
7. Actively participate in the Asset Management and Chargeback programs
8. Manage Software consents and hardware maintenance transfer
9. Perform a wall to wall inventory of In-Scope devices
10. Work with the MSI to implement the Chargeback system and processes
11. Perform employee staffing and transition

Transition Governance Setup. The Service Provider will work with the MSI to establish Transition governance under the Service Provider Transition Project Management Office that will align with the MSI and the DIR DCS Transition PMO structures. The Service Provider will ensure processes and tools are implemented to support Transition change control, schedule, quality, communications, risk and issues management.

MSI Integration. The Service Provider will work closely with the MSI to manage the milestones and dependencies in **Attachment 19-A** to ensure timely and effective integration of tools and processes such as the MSI systems management tools, MSI service support tools and development of the Service Management Manual.

Integration activities will include:

- Joint development of an organizational change management plan: Starting in Phase I of Transition, the Service Provider will work with the MSI to identify, communicate and monitor organizational changes. As a part of Transition planning, the Service Provider will work with the MSI and DIR to identify stakeholders and the impacts to those stakeholders. Information describing the changes and impact will be communicated to the stakeholders as early as possible. The Service Provider will work with the MSI to monitor the changes to ensure outliers are detected early and managed appropriately.
- Working with the MSI to align Transition timeframes: The Service Provider will work with the MSI to develop an integrated project plan. The Service Provider will start with comparing the milestone deliverables from the MSI and Service Provider to ensure dependencies can be met. After this exercise, the Service Provider will work with the MSI's Transition manager to develop a common plan structure and work Breakdown Structure. Activities, tasks, duration and resources from MSI and Service Provider organizations will be added to the common structure until the MSI and Service Provider agree with the level of detail. With this approach, both the MSI and Service Provider will be driving to a single plan.

- Support for configuration of MSI's ITSM system: During Phase I of Transition the Service Provider will work closely with the MSI's ITSM team to provide the configuration requirements as they setup and configure the ITSM tool. The Service Provider will deliver to the MSI the business configuration requirements that the Service Provider needs the MSI to setup.
- Support for integration into MSI's ITSM system: During Phase I of Transition the Service Provider will integrate the appropriate event monitoring tools into Netcool and work with the MSI to integrate Netcool into ITSM for auto-generation of tickets. The Service Provider will provide the integration definitions to the MSI and expects for the MSI to apply those definitions to their ITSM tool.
- Participate in Tools and Processes training: The Service Provider will work with the MSI to ensure that all Service Provider employees on this account participate in the appropriate training delivered by the MSI. For new training content that is required for day one operations, the Service Provider will work with the Incumbent Service Provider to ensure the re-badged employees have an opportunity to take that training prior to Commencement. If re-badged employees are unable to participate in the MSI delivered training during Phase I of Transition, the Service Provider will ensure that training is delivered to those employees during Phase II of Transition.
- Support in the development of the OLAs: The Service Provider will work in coordination with the MSI to develop Operating Level Agreements (OLAs) that provide a structure to ensure core processes are operating smoothly, efficiently and giving the DCS Service Providers an early warning to prevent a potential service disruption. As a part of Phase I Transition, the Service Provider will work with the MSI on developing the key OLAs that need to be in place for Commencement. A governance structure will be developed that will define how OLAs are managed, reviewed, measured and maintained throughout the Term of the Agreement.

Complete Security Transition Activities. To maintain continuity of Services at Commencement, Service Provider will provide training to Service Provider's employees and subcontractors on security policies during Phase I Transition. The Service Provider will also complete the following activities as part of Phase I Transition:

- **Security Risk and Vulnerability Assessment.** The Service Provider will conduct its standard security risk assessment on the In-Scope systems, an architecture review, and a vulnerability assessment. This assessment results in a report with recommendations for meeting the Service Provider's baseline security standard.
- **Security Training.** The Service Provider's security team will collaborate with the MSI to participate in the Security Program in **Exhibit 2**. The Service Provider and the MSI will develop security awareness training content consisting of MSI's Security Plan documentation, DIR and DIR Customers' security policy guides and Service Provider's employee security standards. Training will be mandatory for all Service Provider

employees, contractors and subcontractors assigned to work on the Data Center Services program. Appropriate levels of training will be designated and tracked for compliance based on the specific area the employee will be working in. The tracking of both an individual's current training status and overall attainment of group training goals will be tracked and reported in the security clearance database. These levels will range from general security awareness that all employees will participate in to task-specific security and governance requirements targeted at operations, specialist, DIR Customer specific regulations, or working rules needed for compliance with state or federal mandates unique to certain DIR Customers. This training will be delivered both during the new hire process, and post Commencement on a regular schedule to be determined during Transition as new updates become necessary.

- **Security Plan.** During Phase II of Transition the Service Provider's security team will work with the MSI to create a Security Plan per the requirements of **Exhibit 2** and **Exhibit 3**. The Service Provider will begin work on draft policy and procedure documents collectively known as the Security Plan. The Service Provider will use best practice International Organization for Standardization security standards along with past engagement experience to provide an outline that will address but will not be limited to the following: security strategy and technology roadmaps, security operations procedures, standard hardware and software security configurations, physical security policies and procedures, security incident management, private and protected data use standards, and audit procedures and reporting standards. This set of documents will be used as the foundation of the Service Provider's master security plan for Data Center Services operations which will be reviewed and updated on an annual basis.
- **On-boarding and off-boarding.** The Service Provider will conduct required background checks for its employees working on the Services and will work with the MSI to include its support staff in the MSI's security clearance database. The Service Provider will use the MSI's security clearance database as the source of record for the employees that should have access to various systems. Upon receiving validation from the MSI's security clearance database (based on passing of the background check as well as agency-specific requirements), the Service Provider will grant access to employees via its identity management system. Where appropriate, the Service Provider will use its identity management tool to manage access to the systems requiring access by its employees. For systems where the Service Provider is unable to use its identity management system, the Service Provider will assign staff to manage the access. The Service Provider will train its employees on their responsibilities within the Agreement. For logical and physical access to DIR Customers' facilities and environments not managed by the Service Provider, the DIR Customer's security access request process will be followed. For off-boarding, the Service Provider will update the MSI's security clearance database with the status of the employee and concurrently update its identity management tool to ensure the access is revoked. The Service Provider will also immediately notify DIR Customers of any logical or physical access deletions required at DIR Customer managed facilities and environments. The

Service Provider will perform a monthly reconciliation between the MSI's security clearance database and its identity management tool to ensure they are synched.

Complete Disaster Recovery Transition Activities. The Service Provider will conduct knowledge transfer during Phase I of Transition, including review of DIR Customers' DR plans and review of Third Party DR contracts. Consistent with the requirements of **Exhibit 3**, the Service Provider will also update the DR plan contact information and any changes made in the first six (6) months of Transition, by Commencement. The Service Provider will also support the MSI with their deliverable Disaster Recovery Gap Analysis by providing Application DR status data and mapping.

Complete Business Continuity Planning Activities. During Phase I of Transition the Service Provider will develop a Business Continuity Plan to address Crisis Management for its services and personnel should a Disaster occur. The plan will ensure that personnel at all locations receive equal access to data required to deliver the Services in case of Disaster. The plan will address how the Service Provider will coordinate and work with the MSI to ensure that all information is available as appropriate. Technical documentation in the repository will contain the following information:

- Documented personnel information, tasks, assignments, processes, and resources used to respond to any short- or long-term business interruption affecting any Service Provider Facilities in **Attachment 7-B**.
- The steps and recovery strategies required for continuing business and fulfilling its responsibility to DIR and DIR Customers if a business interruption event occurs
- Designated team leaders, alternate leaders, and members, including the MSI and other DCS service providers as required
- DIR and the Service Provider's internal communication plans and escalation procedures

Complete Service Management Manual Documentation. The Service Provider will collaborate with the MSI to complete the Service Management Manual in phases per the requirements of **Exhibit 3**. The Service Provider understands that the Service Management Manual is a four (4) tier manual consisting of: Policies (Tier 1), Processes (Tier 2), Procedures (Tier 3), and Work Instructions (Tier 4). The Service Provider also understands that the MSI is accountable for developing the contents of Tiers 1 – 3 with Service Provider's collaboration and that the Service Provider is accountable for the content of Tier 4 where documents such as the DR Technical Recovery Guides and operations run books reside. The Service Provider will update Tier 4 documentation by performing knowledge transfer with the Incumbent Service Provider and DIR Customers during Phase I of Transition and documenting any new information received. The Service Provider expects that final versions of the Service Management Manual will be stored on the Portal.

Software Consent and Hardware Maintenance. For In-Scope Software and hardware, consistent with the requirements of **Exhibit 12**, the Service Provider will work with DIR, DIR Customers and its OEM vendors to designate the Service Provider as the entity responsible for

managing the Software and hardware. The Service Provider will obtain the Required Consents from DIR and DIR Customers and distribute to the vendors. DIR and DIR Customers will assist, as needed, to solicit responses from the vendors.

During Phase I of Transition, the Service Provider will develop a process to manage the physical and logical elements associated with license management. The Service Provider will use the MSI provided ITSM tool to store, manage and maintain Software licenses in order to effectively manage the lifecycle. The Service Provider will store Software such as operating systems, patches and application software in a Definitive Software Library (DSL) that is particular to the delivery tower. The DSL is used to manage the versioning of Software and associated with the deployment tools so Software can be effectively deployed and managed. In addition to the DSL, the Service Provider will establish a Definitive Media Library (DML) for the storage of physical media associated with Software. This storage will be locked cabinets in the ADC and SDC which will provide a secure environment for the media after it is loaded in the DSL should it be needed at a later time.

Inventory. In support of Commencement and the CMDB True-Up requirements, the Service Provider will work with the MSI to complete an initial physical and, where possible, electronic inventory of hardware assets during Phase I. The Service Provider will start by taking a snapshot of the Incumbent Service Providers' existing CMDB (snapshot CMDB). In coordination with DIR Customers, the Service Provider will then send resources to DIR Facilities listed in **Exhibit 7** to perform the physical inventory and reconcile any findings with the snapshot CMDB. Concurrent with the physical inventory process, the Service Provider will install auto-discovery tools at the ADC, SDC, and Legacy Data Centers to start the electronic inventory process. The appliances installed at the Legacy Data Centers will be able to detect systems at the remote locations. The Service Provider will map the information received from the auto-discovery tool with the reconciled physical asset data from the snapshot CMDB. The Service Provider will map this information with the information collected from knowledge transfer (e.g. Application to Server; Application to business priority, Application to DR priority; Server to Service Tier) and provide this mapped information to the MSI for entry into the new CMDB. If the Service Provider encounters issues with the auto-discovery tools, the Service Provider will work with DIR and DIR Customers to identify and resolve the issue. Potential resolution will be opening additional firewall ports, creating routes between network segments or adding more auto-discovery appliances. The Service Provider will also continually cross check the auto-discovered data against the wall-to-wall asset inventory data and both of those data sets are checked against the snapshot CMDB.

Chargeback. The Service Provider will work collaboratively with the MSI to capture the appropriate billable units and ensure accurate information is sent to the MSI's Chargeback tool. The MSI serves as the single source of IT financial information and provides and maintains the Chargeback and utilization tracking system. During phase I of Transition the Service Provider will support the Chargeback process through the following activities:

- Participate in the development and documentation of processes and policies with the MSI, other DCS Service Providers, DIR, and DIR Customers
- Perform detailed review and knowledge transfer of the Incumbent Service Provider's Chargeback processes, tools, and documentation to identify areas where change is required, and then modify the data gathering tools as needed for DCS invoicing and reporting
- Define Chargeback inputs such as:
 - Usage data
 - Asset data
 - Rate tables
 - Hardware Service Charges
 - Software Service Charges
 - Service Level attainment data
 - Project Pool Hours
 - Adjustments
 - Corrections
- Review existing account codes, sub-account codes and the mapping of the account codes to the usage data, make changes as needed
- Develop, implement and test usage collection with overhead removal methods from data source systems such as:
 - EMC IONIX ControlCenter StorageScope
 - Symantec OpsCenter Analytics
 - Bocada
- VMware vCenter Server
- Sev OneMainframe SMF data, DCOLLECT command and tape management systems
- Clarity project management system
- CMDB
- Offsite tape logs
- Email account directory services
- Document usage data mapping to correct account codes, work with MSI to add this data to Chargeback system

- Establish a validation process to ensure input and output of the Chargeback system is accurate
- Develop automated interfaces, where feasible, and required manual processes to effectively integrate the Service Provider's financial systems with those of the MSI
- Develop and produce mock monthly reports prior to Commencement:
 - One monthly invoice for the Service Provider and designated Third Party vendors
 - One month of chargeback data for each DIR customer for the Service provider and designated Third Party vendors.

5.3 Transition by Service Component

The Service Provider's approach to Transition is consistent across Service Components. This section describes the Service Provider's common approach towards the work-streams for the Mainframe, Data Center, Server and Network Service Components.

1. Establish access between the ADC/SDC and the Service Provider's infrastructure
2. Perform knowledge transfer
3. Assess readiness for cutover

Establish Access to the Consolidated Data Centers Environment. At the start of Transition, the Service Provider will order network circuits and equipment required for access to the environment. This access, termed ACSNet, will enable the Service Provider's remote teams to conduct detailed knowledge transfer offsite and is required to commence services from the Service Provider's Dallas Center of Excellence located in Dallas, TX as documented in **Attachment 7-B**. During Transition, the Dallas Center of Excellence is setup as a third Enterprise Command Center (Server Operations, Network Operations, Mainframe Operations, Data Center Operations) support location in addition to the Consolidated Data Centers. It is also required to provide remote access for the Service Provider's employees not physically at the ADC and SDC.

Conduct Knowledge Transfer. The Service Provider plans on implementing a soft touch process that will reduce the number of times a DIR or DIR Customer employee or Incumbent Service Provider employee is required to participate in knowledge transfer activities. The Service Provider will apply commercially reasonable practices to minimize the disruption to staff while conducting knowledge transfer with this staff. To ensure the soft touch process is shared with the MSI, soon after executing the Agreement, the Service Provider will work with the MSI to identify information required as a part of knowledge transfer (by both the MSI and Service Provider) and assign the point of contact to acquire this information. The Service Provider will also identify the location where this information will be stored. By combining the

requirements of MSI and Service Provider knowledge transfer, the Service Provider will reduce the number of disruptions to DIR, DIR Customers and the Incumbent Service Provider.

To ensure that the Service Provider has captured the required knowledge to assume the Services, the Service Provider will execute a knowledge transfer process that consists of three (3) main phases – RFO Due Diligence, discovery (initial knowledge transfer) and detailed knowledge transfer. Information collected from the RFO Due Diligence will be made available to the MSI. As a part of the discovery phase, the Service Provider’s technicians will assess the information acquired from the RFO Due Diligence and identify any gaps that exist. Based on this assessment, the Service Provider will schedule discovery sessions with the Incumbent Service Provider to help fill in the gaps. As part of knowledge transfer, the Service Provider’s requests will include but are not limited to run-books, processes, and applications and systems DR documentation. Depending on the quality of information received from the Incumbent Service Provider, the Service Provider may also have a requirement to meet with DIR and DIR Customers to obtain application-specific support information (e.g. job re-start procedure, information to populate the CMDB and map each server to the appropriate service tier). During the discovery process, the Service Provider will also be performing the asset inventory (physical and logical) to leverage the inventory information to fill in gaps that may still exist.

During the detailed knowledge transfer phase, for areas where the Service Provider is not re-badging Incumbent Service Provider resources or the Service Provider is not comfortable with the level of information already collected, the Service Provider’s operators will engage in job shadowing and reverse shadowing. In job shadowing, Service Provider staff will sit face-to-face with the employees performing the work through the 24-hour shift to ensure that daily, month-end, and quarter-end processes are captured. In reverse shadowing, the Service Provider takes primary control of the environment under supervision of Incumbent Service Provider support staff. The Service Provider’s staff will be onsite, as appropriate, for these knowledge transfer processes.

Throughout this entire process, the Service Provider’s knowledge transfer lead will document the knowledge, including updates to run books, and upload documented information in the Portal. The Service Provider will work closely with the MSI to ensure applicable work instructions and run-book content are integrated in the Service Management Manual. The positions and roles (as quantified in **Attachment 5-B**) the Service Provider plans to engage with the Incumbent Service Provider include, but are not limited to: Operating System Administrators, Database Administrators, Production Control Administrators, Command Center Operators, Application Support, Service Level Tools Administrators, Backup Administrators, Storage Administrators, Service Delivery Managers, Solution Architects, Disaster Recovery Managers and IT Security Administrators.

Assess Transition Readiness and Cutover to Service Provider. The Service Provider will continually review Transition progress. The Service Provider will work with the MSI to ensure the tools and processes are fully integrated prior to Commencement and submit the formal Transition Readiness Report prior to the Commencement Date per the requirements of **Exhibit**

3. To test each Service Provider team's readiness and test sufficient integration with the MSI, the Service Provider will include a pilot cutover in the Phase I Transition Plan. Detailed plans for the pilot will be developed and approved by the appropriate Data Center Services governance committee.

At cutover, the Service Provider expects that the MSI will establish and manage a Service Provider Transition PMO cutover war room to monitor the progress of activities and ensure all resources are available for any issues that may arise. This cutover war room will send status updates on an hourly basis, or as defined in the cutover plan, until the cutover activities are complete. If the MSI is unable to setup this war room, the Service Provider is prepared to set it up and manage it to ensure successful cutover. The SPT PMO cutover war room will coordinate all activities with the DIR Transition PMO. The leader of the war room (Service Provider or MSI) will execute a plan that includes the activities that need to happen, the resources that need to perform each activity and when on the schedule they needed to be performed.

5.3.1 Mainframe Service Component Transition

In addition to the services outlined in Section 5.3, the Service Provider will perform the following Transition services for Mainframe Services.

Service Management Tools. During Phase I of Transition, the Service Provider will obtain access to the monitoring and management tools installed on DIR and DIR Customer's systems. In Phase II, the Service Provider will review thresholds and identify any changes required to meet SLAs, including installation of new tools if needed. The Service Provider will provide a service measurement tools list (used to monitor and measure SLA compliance) 30 days prior to Commencement. There is no impact to the Service Provider's solution if it is unable to gain access to the Mainframe tools prior to Commencement.

5.3.2 Server Service Component Transition

In addition to the services outlined in Section 5.3, the Service Provider will perform the following Transition services for Server Services.

Service Management Tools. During Phase I of Transition, the Service Provider will deploy and manage tools in the Server environment to support Event Management, Configuration Management, Performance Management, Backup and Recovery and Security. The Service Provider will perform two gap analyses: 1) identify the servers without tools; and 2) a threshold analysis for the tools currently deployed. The Service Provider will work with DIR and DIR Customers to prioritize critical servers lacking tools for Phase I tool deployment. Tools will be installed on all remaining servers during Phase II. As appropriate, the tools will be integrated

into its Event correlation system which will be integrated into the MSI ITSM's tool for auto-ticketing. To deploy the tools, the Service Provider will create tool packages (both agent based and agentless) and test the packages in the Service Provider labs against the operating systems that these packages will be installed on. Upon successful completion of the testing, approved change tickets, and administrative access granted to the systems, the Service Provider's technicians will modify each system with the appropriate package. This approach will ensure that only the right software agents are applied to the required systems and that the right testing has been performed with that agent and operating system combination. If the Service Provider is unable to install their tools onto systems during Phase I, at Commencement the Service Provider will manage the systems as they are managed by the Incumbent Service Provider and start the tools deployment during Phase II of Transition. For systems with no monitoring, the Service Provider will be made aware of outages when DIR or DIR Customers have a problem and call into the Service Desk.

The Service Provider also understands that some systems may not have the capacity to accept additional tools. In this case, the Service Provider will manage the systems as they are managed by the Incumbent Service Provider until they are consolidated or refreshed.

- **Event Management:** To ensure no service interruption, the Service Provider will assume management of the Tivoli Monitoring tool. For systems that are not managed by Tivoli, the Service Provider will deploy its monitoring tool(s) to those systems so they can be monitored. The configuration for Event Management will be included in the tool package and that package will only be applied to systems that are not monitored by the Incumbent Service Provider. The Service Provider plans to work with the Incumbent Service Provider during Transition Phase I to have the Tivoli Event Management system send the Incumbent Service Provider's alerts into the Service Provider's Event correlation tool for auto-ticketing.
- **Configuration Management:** The Service Provider will deploy a Configuration Management tool. This tool will be applied to all systems that are managed by the Service Provider and are supported by the OEM vendor. The Service Provider's Auto-Discovery tool, BMC ADDM, will start being deployed during Phase I for Asset Inventory. As ADDM is not expected to support all systems in the environment, ACS plans to utilize other tools to collect the data in situations where ADDM is not successful.
- **Capacity Management:** The Service Provider will deploy a Capacity and Performance Management tool. This tool will be applied to Platinum and Gold servers per **Exhibit 4**.
- **Backup and Recovery:** The Service Provider will rollout Symantec OpsCenter agents to the Servers in the Business Office locations during Phase II. Rollout of this tool to the Legacy Data Centers, ADC and SDC will be performed during Transformation. If the Service Provider is unable to deploy its backup tools prior to Commencement, the Service Provider will utilize existing backup systems until its tools are deployed. For tape management, the Service Provider will assume contractual relationships with the Incumbent Service Provider's off-site media management vendors during Phase I of Transition. The Service

Provider will use these and other off-site media vendors to provide the storage and management of media for Legacy Data Centers and Business Offices. The Service Provider will provide a plan to define the implementation schedule of off-site media rotation and LDCs and remote sites. The plan will include daily, weekly, monthly and annual processes governing the movement, management and auditing of media and vendor activities to ensure media is kept in a secure and managed location.

- Security: The Service Provider will manage existing security tools in place until license expiration upon which the Service Provider will deploy several tools for a highly secure IT environment for DIR and DIR Customers. During Phase I, the Service Provider will deploy
 - McAfee Enterprise Policy Orchestrator to manage the distributed McAfee agents
 - McAfee Anti-Virus, Anti-Malware, and Anti-Spyware
 - McAfee Host Intrusion Prevention Systems (HIPS)
 - McAfee Intrushield Network Intrusion Detection Systems (NIDS)
 - RSA Envision Security Incident and Event Management (SIEM)
 - Critical Watch Vulnerability Assessment

The Service Provider will work closely with the Incumbent Service Provider to manage the applicable milestones and dependencies in **Attachment 19-A** to ensure timely and effective deployment of tools.

Where tools cannot be installed in Phase I, the Service Provider will delay the installation of the tools until Phase II of Transition and utilize the processes and tools that are in place. Phase II tools deployment will be completed by Commencement plus four (4) months unless agreed to by DIR.

At Commencement, the Service Provider will disable logical access for Incumbent Service Provider staff that will not be rebadged.

In Phase II, the Service Provider will review the thresholds and identify any changes required to meet SLAs, including installation of new tools if needed. Service Provider will uninstall Incumbent Service Provider's tools that are replaced by the Service Provider's tools.

The below chart provides a timeline of the Service Provider's plan for deploying tools to servers in the environment per the Services Tier Matrix.

Completion Timeframe	Included Servers	Net	HW	OS	DB	App	App URL	MW	Capacity
7/1/2012	All existing monitoring will remain in place on 7/1.								
8/1/2012	High/Gold Servers	Yes	Yes	Yes	Yes			Yes	Yes
10/1/2012	Med/Silver Servers	Yes	Yes	Yes	Yes			Yes	
11/1/2012	Low/Bronze Servers	Yes	Yes	Yes					
11/1/2012	High/Gold Servers					Yes	Yes		
Post 11/1/2012	Optional Services				Yes	Yes	Yes	Yes	
Assumptions									
Agencies will permit ACS to deploy the tools on the proposed schedule.									
Agencies will work with ACS to identify applications to be monitored on Gold servers, as well as optional services.									
The ability to perform application monitoring will be in place by the agreed upon date in 19A, but actual monitoring of the application(s) will be contingent upon the agencies providing the applicable data to ACS.									
Definitions									
Network	Server IP ping with alerts								
Hardware	Server (Up/Down, Hardware specific errors, component monitoring, CPU, Disk Memory, Components of a server)								
Operating System	Server Capacity Threshold Monitoring (CPU, Memory, filesystem and OS disk).								
Database	DB up/down, DB free space, DB status, etc.								
Application	Any process required to support the Application. Process Up/Down, URL website availability, application file system capacity and availability								
Application URL	URL website availability								
Middleware	Middleware process Up/Down, application file system capacity and availability where the standard tools are capable of such monitoring.								
Capacity	Capacity management service that reports historical trends of key server resources.								

5.3.3 Data Center Service Component Transition

In addition to the services outlined in Section 5.3, the Service Provider will perform the following Transition services for Data Center Services.

Cable Infrastructure and Management. The Service will implement the Rackwise Data Center Management (DCM) software tool during Transition Phase I to support the maintenance of equipment layouts, rack elevations and cable management systems at the Consolidated Data Centers. Existing cable infrastructure records for the Consolidated Data Centers will be validated and imported into the Rackwise DCM tool during Transition Phase I. Data center procedures for cable management will be updated to incorporate the use of Rackwise DCM to support cable management and the data center staff trained in use of Rackwise DCM to support data center planning for equipment installation and cable management.

Tape library, management, and integration with offsite media management. The Service Provider will take control of the off-site media services supporting the Consolidated Data Centers at Commencement and will continue to utilize the Incumbent Service Provider's Webscan system to support tracking of on-site and offsite media and offsite media rotations for the Consolidated Data Centers.

The Service Provider will conduct a physical inventory of the external storage media associated with the Consolidated Data Centers (both on-site media and media at the off-site storage vault) at Commencement. The inventory results will be reconciled with the Incumbent Service Provider's existing Webscan system to verify that all of the media associated with the Consolidated Data Centers is accounted for. The Webscan media reporting from this inventory will be used by the Mainframe and Server towers to support reconciliation the mainframe and server tape management system records.

Transition Support for physical security at the ADC and SDC. The Service Provider will coordinate advance badging of staff requiring physical access to the ADC and SDC facilities prior to service Commencement. Management approval and background check clearance confirmation using the security clearance database will be requisite for badging at both the ADC and SDC facilities.

Prior to service Commencement, the Service Provider will review the facility access lists at both the ADC and SDC facilities to identify Incumbent Service Provider staff that will not be rebadged at Commencement.

At service Commencement, at the ADC and SDC, the Service Provider will collect access badges from and revoke building access credentials for Incumbent Service Provider staff that will not be rebadged. Security staff at both facilities will be on heightened alert enforcing the requirement for all staff and visitors to display facility access badges at all times. Security staff will be on-duty 24x7 from service Commencement forward to enforce physical security procedures at the Consolidated Data Centers, monitor alarms and CCTV facility cameras, and control facility visitor access per Service Management Manual procedures.

5.3.4 Network Service Component Transition

In addition to the services outlined in Section 5.3, the Service Provider will perform the following Transition services for Network Services.

Service Management Tools. The Service Provider plans to deploy and manage tools in the network environment that will support Event Management; Configuration Management; Performance Management; and Security. As appropriate, the tools will be integrated into the Service Provider's Event correlation system which will be integrated into the MSI ITSM's tool for auto-ticketing. The tools the Service Provider intends to deploy during Phase I are agentless tools that will only need SNMP read strings and ICMP access to the network devices. To deploy the tools, the Service Provider will work with the Incumbent Service Provider to install appliances in the ADC or SDC, as appropriate. The Service Provider will work with the Incumbent Service Provider's network administrator to obtain cabinet space to install appliances, IP addresses to connect to the LAN, open the appropriate firewall ports and SNMP read-strings to the devices.

- **Event Management:** Service Provider will deploy SevOne network management tool for device event management. This tool will be deployed in Phase I and will be ready for operations at Commencement
- **Configuration Management:** Service Provider will deploy EMC Voyence for Network Configuration Management tool during phase I.
- **Performance Management:** Service Provider will deploy Apparent Networks AppCritical for performance management during phase I.
- **Security:** In order to provide a smooth transition from the existing security infrastructure to the proposed security solution, the Service Provider will implement a phase-in, phase-out approach. During Phase I of Transition, the Service Provider will establish a takeover in place and knowledge transfer strategy for the security tools supported by the Incumbent Service Provider. Until each tool reaches its contract end date or the appropriate master security infrastructure tools the Service Provider is implementing are in place and tested, the Service Provider plans to manage as is under a Transition security operation plan.
- **Intrusion Detection Services and Intrusion Prevention System:** During Phase II, the Service Provider will replace the Incumbent Service Provider's intrusion detection service with the new McAfee Intrushield appliance architecture as described in the solution documents.
- **Anti-virus; Host-Based Intrusion Protection Service (HIPS):** The Service Provider will leave in place and manage the existing agent based Anti-virus and HIPS enterprise command infrastructure while in parallel build the future McAfee Enterprise Orchestration management environment. As the Incumbent Service Provider's anti-virus contract expires, the Service Provider will transition off all agent based services to the new platform. The Service Provider will have the replacement infrastructure in place at Commencement to provide services to any servers placed into the virtual environment, and to address refreshes as they occur based on the midrange refresh cycles. The various existing Server-based email anti-virus platforms used by the DIR Customers today will be managed as-is during Transition and through the end of each contract license term. During that time the Transition Risk and Vulnerability Assessment will be used to identify any gaps that might exist, and to make recommendations for a possible centralized datacenter based replacement that can be implemented as part of Transformation.
- **Security Incident and Event Management and log monitoring:** The Service Provider will implement the centralized security log collection, storage, and correlation environment during Phase I of Transition. Concurrent with the activities of installing monitoring tools on DIR and DIR Customer's systems, the Service Provider will configure those Systems to log to the RSA envision SIEM so that at Commencement, the Service Provider can start full security log monitoring and event management. For those Systems not ready to transition at Commencement, the Service Provider will continue to support the Tivoli solution in place.
- **Vulnerability Management:** The Service Provider will implement the CriticalWatch platform for vulnerability management. The Security Risk and Vulnerability Assessment

performed during Phase I of Transition will be used to identify specialized vulnerability scanning systems in place today that are used to meet unique regulatory or DIR Customer-specific solutions. The Service Provider will support these solutions as-is until the Service Provider can make an assessment of the solution's function and capabilities against the long term IT plan.

The Service Provider will work closely with the Incumbent Service Provider to manage the applicable milestones and dependencies in **Attachment 19-A** to ensure timely and effective deployment of tools.

Where tools cannot be installed in Phase I, the Service Provider will delay the installation of the tools until Phase II of Transition and utilize the Incumbent Service Provider's processes and tools. Phase II tools deployment will be completed by Commencement plus three (3) months unless agreed to by DIR.

6. SERVICE PROVIDER TRANSITION ROLES AND GOVERNANCE ALIGNMENT

The Service Provider has a Transition team dedicated to the Data Center Services Agreement. The Service Provider's Transition Director will lead the Service Provider Transition team. Reporting into the Transition Director are two teams, an MSI interface team and an operations readiness team. This organization will align to MSI and DCS program governance structures, including the SPT PMO and the DIR DCS Transition PMO.

The MSI interface team will focus on activities around integrating tools and processes with the MSI. The operations readiness team will focus on activities around transitioning services from the Incumbent Service Provider to the Service Provider. Figure 2 is a visual representation of the Transition organization.

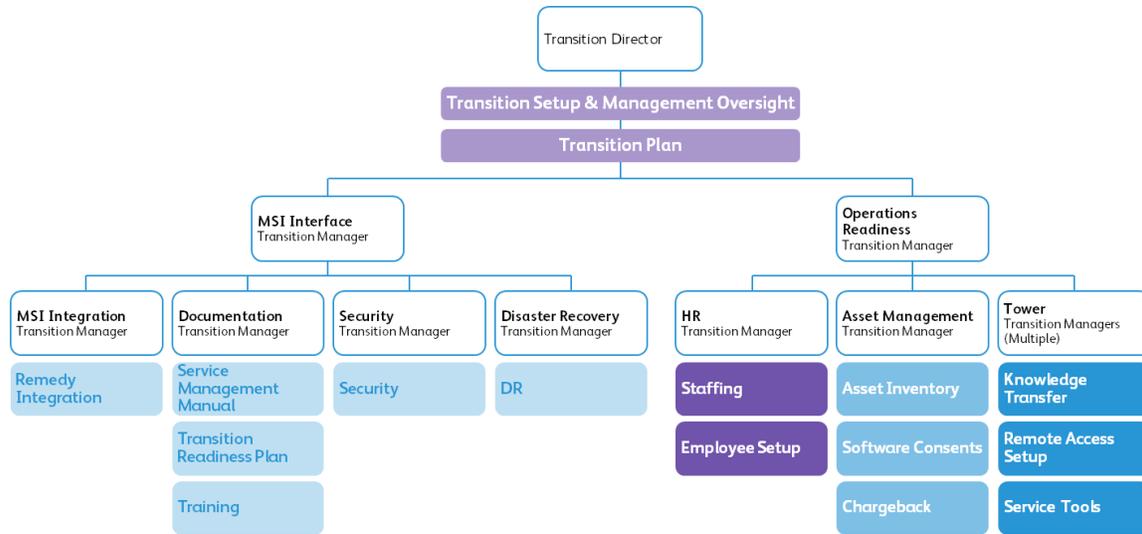


Figure 2. Transition Management Team

7. QUALITY CONTROL AND GENERAL RISK MITIGATION

Quality Control

Service Provider will work with the MSI and align with the MSI’s Integrated Quality Management Plan. At a minimum, the Service Provider will ensure that there are processes around quality planning, Quality Assurance and quality control. These processes will govern the project management deliverables as well as the technical deliverables to DIR and DIR Customers.

Clearly defined Acceptance Criteria for the Transition Milestone Deliverables have been developed and are included in **Attachment 19-A**. The Acceptance Criteria, where appropriate, includes the testing procedures and criteria for testing. Prior to a deliverable being submitted to DIR as complete, appropriate stakeholders will have an opportunity to provide input to the deliverable. Final deliverables will be approved by the designated approver in **Attachment 19-A**.

Risk Mitigation

Consistent with the Service Provider’s approach to quality, the Service Provider intends to work with the MSI and align with their Risks and Issues Management Plan. Per **Attachment 19-A**, the Service Provider has identified risks and will ensure that these risks, as well as additional ones identified, are tracked in a common repository so Service Provider, MSI, DIR and DIR Customers are aware of the current status of the risks. Service Provider will also ensure that those risks and issues are proactively communicated to the right level of management for immediate resolution and mitigation.

8. COMMUNICATIONS

Early in the process, the Service Provider will work with stakeholders to define roles and responsibilities as well as provide input to the Communications Plan provided by the MSI to ensure the right audience is being communicated to within a timely fashion. The outcome of these activities will define the communications interfaces for the Service Provider, the MSI, the Incumbent Service Provider, DIR, and DIR Customers.

Service Provider will communicate through formal and informal methods. Communications will take place through regularly scheduled meetings, impromptu meetings for urgent items, emails and status reports.

Service Provider will participate in Transition meetings established by the MSI as well as setup meetings identified by Service Provider as necessary for success. At a minimum, the Service Provider envisions the teams being in regular contact with the MSI, DIR, DIR Customers, Transition Solution Group, and the Incumbent Service Provider.

Figure 3 below provides a preliminary view of the types of communications and frequency of communications the Service Provider plans to have with DIR and the MSI.

Communication	Frequency	Purpose	Stakeholders
Executive Status Meeting	Weekly	Executive Status Update to steering committee and Executive Leadership	<ul style="list-style-type: none"> Executive Sponsors Transition Executives Project Manager Service Provider Account Executive MSI Account Executive
Transition Leadership Meeting	Weekly	Transition Status Update to Transition Executive Team	<ul style="list-style-type: none"> DIR Transition Executive MSI Transition Executive Service Provider Transition Executive Transition Managers
Joint Program Team Meeting	Multiple times per week (To be determined by the team)	All towers working session <ul style="list-style-type: none"> Action Items review Risk/Issues list review 	<ul style="list-style-type: none"> DIR Transition Executive* MSI Transition Executive* Service Provider Transition Executive* MSI Transition Managers Service Provider Transition Managers SME Leads as needed
Workstream Meetings	Variable (Workstream specific)	Tower specific work session <ul style="list-style-type: none"> Action Items review Risk/Issues list review 	<ul style="list-style-type: none"> MSI Transition Managers Service Provider Transition Managers SME Leads

*Optional attendees

Figure 3. Communications Plan