

State of Texas
Department of Information Resources



Exhibit 2.1.1

Cross-Functional Services Statement of Work

Texas.gov Services

DIR-ESS-TGOV-SVCS-254

Table of Contents

1	INTRODUCTION	2
1.1	Operating Model	2
1.2	Document Overview	2
1.3	Shared Services Systems and Processes.....	3
2	MARKETPLACE	5
2.1	Portal	5
2.2	Service Catalog Management.....	5
2.3	IT Service Desk and Constituent Help Desk.....	5
2.4	Outreach and Growth	7
3	SERVICE MANAGEMENT	7
3.1	Incident Management	8
3.2	Problem Management	9
3.3	Information Security Management.....	10
3.4	Request Management and Fulfillment	15
3.5	Change Management.....	19
3.6	Asset Inventory and Management.....	20
3.7	Software License Management	21
3.8	Configuration Management.....	23
3.9	IT Service Continuity Management	25
3.10	Project Management.....	25
3.11	Release Management.....	26
4	BUSINESS MANAGEMENT	26
4.1	Operational Intelligence	26
4.2	Service Level Management.....	27
4.3	IT Financial Management	28
4.4	Capacity Management.....	29
4.5	Refresh and Technical Currency	30

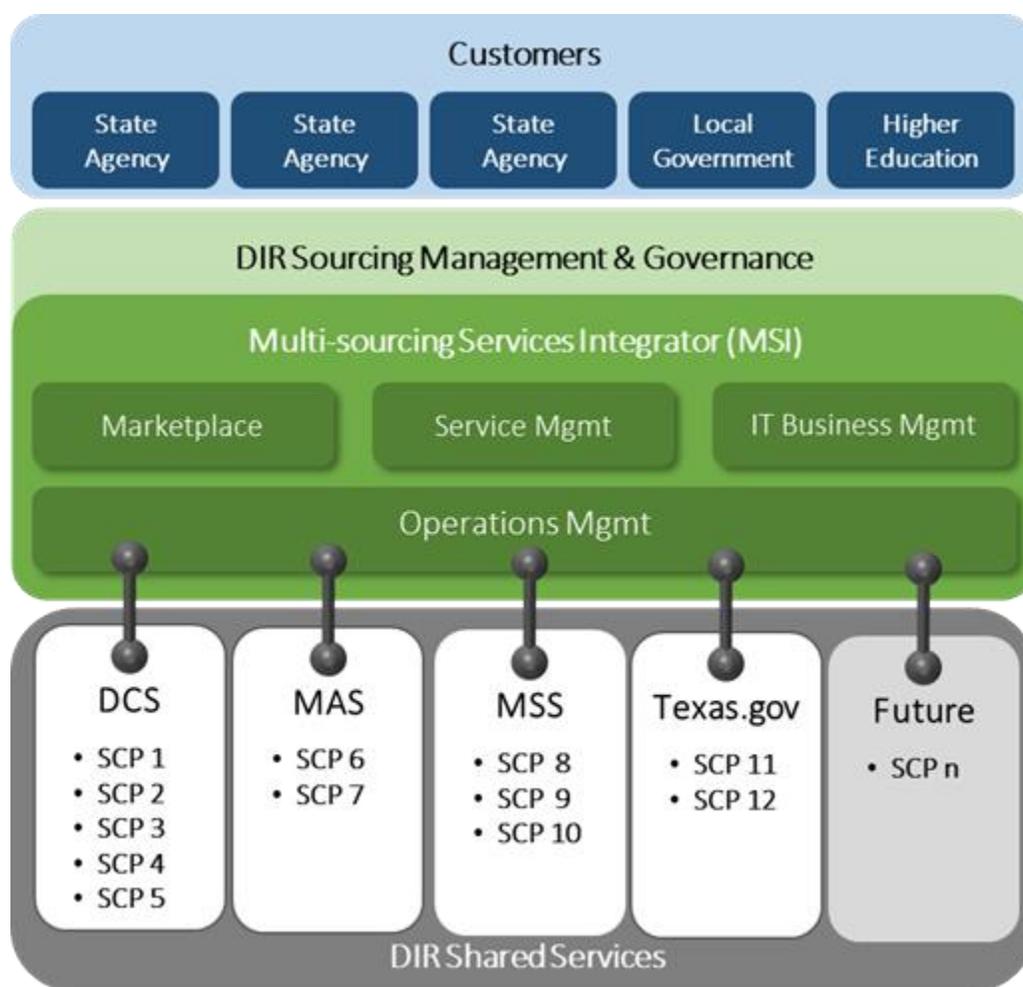
1 INTRODUCTION

1.1 Operating Model

This Exhibit contains specific functional requirements that all Service Component Providers (SCPs) must meet in order to perform the requested Services and responsibilities defined in **Exhibit 2.0 Service Model**. SCPs must integrate with DIR’s Multi-sourcing Services Integrator (MSI).

DIR contracts with multiple SCPs to deliver shared technology services to DIR Customers. Those services are integrated into a common service delivery model by DIR’s MSI. The MSI provides the systems, processes and service delivery oversight necessary to ensure consistent, quality service delivery. Figure 1 below depicts the relationships between SCPs and the MSI.

Figure 1



1.2 Document Overview

This document contains Service Management categories of responsibilities that apply to the delivery of Services. These categories are considered cross-functional in that they are functions which cross all SCPs.

1.3 Shared Services Systems and Processes

DIR bases its service management practices on the Information Technology Infrastructure Library (ITIL), which focuses on the service management lifecycle and the linkages between service management components. The Successful Respondent shall be responsible for using management practices complying with the ITIL framework in cooperation with and as established by the MSI.

1.3.1 Shared Services Processes

The Successful Respondent shall, at a minimum:

- 1.3.1.1 Conform and deliver to a set of processes based on ITIL guidance to enable consistent management of IT services seamlessly across the MSI and among SCPs.
- 1.3.1.2 Ensure that processes effectively integrate with the processes, functions and roles deployed within and used by DIR Customers, MSI, and the other SCPs.
- 1.3.1.3 Design processes and procedures to enable the effective monitoring and reporting of Successful Respondent's Services.
- 1.3.1.4 Coordinate the execution of Successful Respondent processes across DIR Customers and with the MSI to ensure all the individual components that make up the required Services are managed in an end-to-end manner.
- 1.3.1.5 Document Successful Respondent-level processes and procedures in the integrated Service Management Manual (SMM).
- 1.3.1.6 Deploy any necessary processes, procedures, and controls to provide effective end-to-end management, monitoring, and reporting of the Services.
- 1.3.1.7 Deploy and integrate any tools and systems necessary to enable such processes, procedures, and controls.
- 1.3.1.8 Implement change and configuration management for systems, services, and components managed by Successful Respondent.
- 1.3.1.9 Maintain security Tools to meet performance standards, processes and policy requirements, to maximize efficiency, and to minimize outages, as necessary.
- 1.3.1.10 Provide audit logs for any systems managed by the Successful Respondent.

1.3.2 Shared Services Documentation

All documentation maintained by the Successful Respondent shall be subject to approval by DIR and will conform to the documentation standards and format provided by the MSI and agreed upon between DIR and the Successful Respondent. The Successful Respondent shall develop documentation in accordance with the requirements in **Exhibit 1.3 Service Management Manual**.

The Successful Respondent shall, at a minimum:

- 1.3.2.1 Ensure that Successful Respondent's operations documentation related to the Services is up to date, accurate, and posted in the MSI's SMM.
 - 1.3.2.1.1 Identify owners (business, operational, quality assurance, and engineering) of documentation.
 - 1.3.2.1.2 Link Systems documentation to architectural standards.

- 1.3.2.1.3 Identify DIR Data to the associated System(s) and the associated security risk classification.
- 1.3.2.1.4 Provide access to architecture and design documentation for Systems and services managed by Successful Respondent.
- 1.3.2.1.5 Create and maintain current documentation as required (e.g., support documentation).
- 1.3.2.2 Develop and maintain documentation on all Operations procedures, Services, Equipment, and Software for which Successful Respondent is responsible according to the standard SMM format.
- 1.3.2.3 Make all documentation available electronically.
- 1.3.2.4 Validate documentation annually for completeness and accuracy, and verify that all documentation is present, organized, readable, and updated in accordance with agreed upon schedule.
- 1.3.2.5 Participate in the reporting of validation findings to DIR and DIR Customers on a regular basis, and where it is determined that documentation is inaccurate (e.g., erroneous or out of date), correct and replace such documentation.
- 1.3.2.6 Update the SMM according to schedule described for the Critical Deliverables in **Exhibit 3.3 Critical Deliverables**.

1.3.3 Training & Education

The Successful Respondent shall, at a minimum:

- 1.3.3.1 Support the MSI as appropriate to ensure the proper training on Service Management Systems and other tools, including the supporting processes, for Successful Respondent personnel.
- 1.3.3.2 Develop applicable training content and coordinate with the MSI to load and manage within the MSI-provided Learning Management System (LMS).
- 1.3.3.3 Customize such applicable Successful Respondent training to be specific to the Authorized Users for the Services within the DIR environment.
- 1.3.3.4 Schedule and provide training on the applicable Service Component for new Successful Respondent Users based on the needs of DIR or DIR Customers. Create and maintain training material for Successful Respondent staff that includes at least the following information: The Services provided; the value of Services to DIR; the financial structure of charges; overview of DIR and DIR Customers; DIR Security Policies; orientation to all applicable laws and regulations (e.g., 1 TAC 202, HIPAA); the location of document stores; and the structure and location of the SMM.
- 1.3.3.5 Ensure that all staff interacting with DIR or DIR Customers have reviewed the minimum set of documentation as defined by the Successful Respondent in the **Exhibit 3.3 Critical Deliverables** for **Transition Readiness and Transition Plan**.
- 1.3.3.6 Upon request, Successful Respondent shall provide such documentation and training to DIR and DIR Customers as specified by DIR.

2 MARKETPLACE

2.1 Portal

The Successful Respondent must leverage the MSI-provided Portal to provide integrated DIR and DIR Customer communications and reporting. Reporting functions and specific operational reports are defined in **Exhibit 3 Performance Model**, and **Exhibit 3.4-A Reports**.

The Successful Respondent shall, at a minimum:

- 2.1.1.1 Provide the MSI with the reports and communication content to be posted.
- 2.1.1.2 Provide reports and communication content in the format and standards required of the MSI's online portal.
- 2.1.1.3 Adhere to established processes as documented in the SMM.

2.2 Service Catalog Management

The MSI provides the Service Catalog tool for DIR Customers to request Services from the Successful Respondent.

The Successful Respondent shall, at a minimum:

- 2.2.1.1 Coordinate with the MSI to ensure integration of Successful Respondent Services into the Service Catalog.
- 2.2.1.2 Support the MSI to categorize and normalize Service Catalog content.
- 2.2.1.3 Support the MSI to determine the approval authority required to obtain the Service.
- 2.2.1.4 Support the MSI to document Service descriptions and dependencies.
- 2.2.1.5 Participate, through the MSI, in regular communications with DIR and DIR Customers on updates to the Service Catalog.
- 2.2.1.6 Respond to Service Catalog requests in accordance with defined processes and Service Level Agreements (SLAs).

2.3 IT Service Desk and Constituent Help Desk

2.3.1 IT Service Desk

Successful Respondent shall be responsible for responding to incidents or requests DIR Customers log with the MSI's Service Desk, in compliance with policies and procedures set forth in the SMM and managed by the MSI.

The MSI's Service Desk shall be the single point of contact for Authorized Users regarding Incidents, which include events that cause or may cause an interruption or reduction of service, as well as for requests for information and requests for services relating to all of DIR's and DIR Customers' IT Services.

The Successful Respondent shall, at a minimum:

- 2.3.1.1 Actively participate with the MSI to develop and document processes.

- 2.3.1.2 Integrate Successful Respondent's Service processes with the Service Desk processes of the MSI, DIR Customer, and authorized Third Party Vendor(s), where the processes interact.
- 2.3.1.3 Actively support the MSI to assure the proper application of Service Desk across all functions and organizations that provide services to DIR Customers.
- 2.3.1.4 Communicate and coordinate the Service Desk processes and policies within Successful Respondent's own organization and DIR Customers.
- 2.3.1.5 Actively participate in defining Service Desk policies and procedures, as approved by DIR, which set the objectives, scope, and principles that ensure the success of the Incident Management processes.
- 2.3.1.6 Provide effective and agreed upon mechanisms for properly complying with the Service Desk policies.
- 2.3.1.7 Manage all Incidents, Service Requests, etc., from Authorized Users relating to Services, including the following:
 - 2.3.1.7.1 Assigning categorization and prioritization codes.
 - 2.3.1.7.2 Communicating with users, keeping them informed of progress, notifying them of impending actions, obtaining appropriate agreement, and in all ways engaging and communicating with them about Successful Respondent activities.
 - 2.3.1.7.3 Closing all resolved Incidents, Service Requests, and other calls.
- 2.3.1.8 Develop and document processes regarding interfaces, interaction, and responsibilities between Level 1 Support personnel, Level 2 Support personnel, and any other internal or external persons or entities that may either submit an Incident or receive an Incident.
- 2.3.1.9 Utilize the Incident Management System provided by the MSI and integrate with the MSI Service Desk, including the use of tools, technology, processes, and procedures.
- 2.3.1.10 Analyze Incident trends and recommend and implement actions, with DIR and DIR Customer(s) approval, to reduce Incidents. Also:
 - 2.3.1.10.1 Provide on-line FAQs and help documentation for common problems.
 - 2.3.1.10.2 Provide the MSI with information necessary to keep Authorized Users regularly updated with alerts advising of any new or changed information.

2.3.2 Constituent Help Desk

The MSI operated Constituent Help Desk is the single point of contact for Constituents regarding Incidents, requests and questions relating to State provided services (i.e., Texas.gov). The citizens contacting this help desk are referred to as Constituent Users.

The Successful Respondent shall be responsible for providing information and scripts to enable the MSI to operate the Constituent Help Desk to support first call resolution. Incidents raised by Constituents that are not resolved by the MSI will be worked according to the IT Service Desk processes.

The Successful Respondent shall, at a minimum:

- 2.3.2.1 Actively participate with the MSI to develop and document processes.

- 2.3.2.2 Integrate Successful Respondent's Service processes with the Constituent Help Desk processes of the MSI, DIR Customer, and authorized Third Party Vendor(s), where the processes interact.
- 2.3.2.3 Actively support the MSI to assure the proper application of Constituent Help Desk across all functions and organizations that provide services to DIR Customers.
- 2.3.2.4 Communicate and coordinate the Constituent Help Desk processes and policies within Successful Respondent's own organization.
- 2.3.2.5 Actively participate in defining Constituent Help Desk policies and procedures, as approved by DIR.
- 2.3.2.6 Provide effective and agreed mechanisms for properly complying with the Constituent Help Desk policies.
- 2.3.2.7 Support the MSI to develop and document processes and knowledge articles regarding applications, interfaces and functionality to enable the MSI to provide effective Constituent Help support to Constituents.
- 2.3.2.8 Analyze Constituent Help request and incident trends relative to the Successful Respondent's scope and recommend and support the MSI implement actions, with DIR and DIR Customer(s) approval, to reduce requests and incidents, including:
 - 2.3.2.8.1 Increase the availability of MSI self-help capability, such as providing on-line FAQs and help documentation for common problems.

2.4 Outreach and Growth

The Successful SCP Respondent shall promote the Services to public sector entities within the State of Texas; including all potential DIR Customers, specifically state agencies, universities and higher education, counties, and municipalities.

Successful SCP Respondent shall, at a minimum:

- 2.4.1.1 Develop and execute against an Outreach Approach, subject to the approval of DIR, that describes how Services are branded and communicated, how stakeholder needs are assessed, what outreach efforts meet those needs, and how satisfaction with Services is measured and improved.
- 2.4.1.2 Provide outreach to current and potential DIR Customers. Successful Respondent shall, at a minimum:
 - 2.4.1.2.1 Collaborate with DIR Customers to understand their needs and to promote the benefits of Texas.gov initiatives.
 - 2.4.1.2.2 Communicate and promote specific service benefits to targeted needs.
 - 2.4.1.2.3 Deliver compelling incentives to DIR Customers to use the Services.
 - 2.4.1.2.4 Build trust through promotion of the benefits, such as ease of use, security, and privacy.
- 2.4.1.3 Participate with Texas.gov Customers in a community that shares knowledge, ideas, and best practices to collaborate across boundaries.

3 SERVICE MANAGEMENT

3.1 Incident Management

Successful Respondent shall, at a minimum:

- 3.1.1.1 Provide Incident Management Services in the form of tier 2 support and tier 3 support. Incident Management is separate and distinct from Security Incident Management.
- 3.1.1.2 Provide knowledge capture and transfer regarding Incident resolution procedures to support the objective of increasing the number of Incidents capable of being resolved by tier 1 support.
- 3.1.1.3 Comply with MSI policies and procedures for Incident Management.
- 3.1.1.4 Coordinate with the MSI to develop and approve Successful Respondent-related Incident Management content in the MSI-managed SMM.
- 3.1.1.5 Utilize the Incident Management System provided by the MSI for all information related to an Incident.
- 3.1.1.6 Provide for training on processes and tools for Incidents and escalations to Successful Respondent Incident Management staff and other relevant resources involved with responding to Incidents.
- 3.1.1.7 Resolve Incidents in accordance with the SMM, knowledge database documents, and configuration database(s).
- 3.1.1.8 Identify and classify Incident severity and handle according to agreed-upon Incident response procedures and assume end-to-end responsibility.
- 3.1.1.9 Escalate Incidents in accordance with the SMM, knowledge database documents, and configuration database(s).
- 3.1.1.10 Provide tier 2 support and tier 3 support, unless tier 3 support is provided by a third-party vendor.
- 3.1.1.11 Participate in Incident review sessions.
- 3.1.1.12 Update the progress of an Incident's resolution within the MSI tracking systems through to final closure.
- 3.1.1.13 Verify that all records (e.g., inventory, asset and configuration management records) are updated to reflect completed and resolved Incidents.
- 3.1.1.14 Document solutions to resolved Incidents in MSI-managed central knowledge base. Accurately update all information pertinent to trouble ticket including general verbiage, codes, etc.
- 3.1.1.15 Determine if an Incident should initiate a Problem investigation (e.g., whether preventive action is necessary to avoid Incident recurrence) and, in conjunction with the appropriate support tier, raise a Problem record to initiate action.
- 3.1.1.16 Conduct follow-up with DIR Customer representative who reported the Incident to verify the Incident was resolved to their satisfaction.
- 3.1.1.17 Integrate the Successful Respondent's Incident Management process with the other service management processes, especially Problem Management, Configuration Management, Service Level Management, and Change Management.

- 3.1.1.18 The Successful Respondent shall utilize the Incident Management System provided by the MSI and integrate such with their Incident Management processes, providing a level of detail that allows for a set of Incident Resolution diagnostics.
- 3.1.1.19 The MSI shall provide the systems, processes and service delivery oversight necessary to ensure consistent, quality service delivery.

3.2 Problem Management

The Successful Respondent shall, at a minimum:

- 3.2.1.1 Provide Problem Management Services in coordination with the MSI Problem Management structure to minimize the adverse impact of Incidents on DIR Customer's business operations.
- 3.2.1.2 Cooperate with the MSI to provide reactive Problem Management Services by diagnosing and solving Problems in response to one or more Incidents that have been reported through Incident Management.
- 3.2.1.3 Provide proactive Problem Management to identify and solve Problems and known errors before Incidents occur, including:
 - 3.2.1.3.1 performing predictive analysis activities, where practical, to identify potential future Problems,
 - 3.2.1.3.2 develop recommended mitigation plans, and
 - 3.2.1.3.3 implement approved corrective mitigation actions and processes.
- 3.2.1.4 Maintain, update, and disseminate information about Problems and the appropriate workarounds and resolutions to reduce the number and impact of Incidents.
- 3.2.1.5 Provide Problem Management Services for all Problems that are determined to be related to the in-scope Services. Successful Respondent shall also provide coordination and assistance to DIR Customer and other Service Component Providers in performing their Problem Management functions related to the in-scope Services.
- 3.2.1.6 Implement resolutions to Problems through the appropriate control procedures, especially Change management, as well as coordinating Problem Management activities with the various teams within Successful Respondent, DIR Customer, MSI and other Service Component Providers responsible for performing Configuration Management, IT Service Continuity Management, and Service Level management activities.
- 3.2.1.7 Coordinate with the MSI to develop and implement processes for Problem Management and root cause analysis (RCA) (e.g., events that trigger an RCA).
- 3.2.1.8 Comply with MSI policies for Problem Management and RCA.
- 3.2.1.9 Participate in Problem Management review meetings.
- 3.2.1.10 Use and update the Problem Management knowledge database managed by the MSI.
- 3.2.1.11 Perform Problem Management activities as set forth in the MSI-managed SMM.
- 3.2.1.12 Coordinate and take responsibility of Problem Management activities of all Problems that reside in Successful Respondent's area of responsibility (e.g., detection, logging, RCA, etc.).

- 3.2.1.13 Conduct proactive trend analysis of Incidents and Problems to identify recurring situations that are or may be indicative of future Problems and points of failure.
- 3.2.1.14 Develop and recommend corrective actions or solutions to address recurring Incidents and Problems or failures, as well as mitigation strategies and actions to avert potential Problems identified through trend analysis.
- 3.2.1.15 Identify, develop, document (in the MSI Problem Management tool), and recommend appropriate workarounds for known errors of unresolved Problems and notify Incident Management and all other appropriate DIR Customer stakeholders of its availability, if approved by DIR Customer.
- 3.2.1.16 Create documentation with recommended corrective actions to resolve a Problem and submit to Change management for review and approval using the MSI provided tool.

3.3 Information Security Management

Successful Respondent's delivery of Information Security Management shall be an integral part of the Services and shall assess all security risks associated with the delivery of Services are appropriately identified, evaluated, assessed and appropriate controls are implemented and maintained.

3.3.1 Information Security Management General Requirements

The Successful Respondent shall, at a minimum:

- 3.3.1.1 Work with the MSI in support of the overall cybersecurity risk management program.
- 3.3.1.2 Work with the MSI to develop and maintain security procedures and Service Responsibility Matrices, physical and logical access strategies, and standards.
- 3.3.1.3 Adhere to the Information Security Management processes as defined in the SMM.
- 3.3.1.4 Work with the MSI to integrate Successful Respondent's security program with DIR's governance risk and compliance program, including at a minimum Incident recording, CMDB, security exception, security plan submission, risk assessment and in integrating Successful Respondent's Security tools directly with the MSI as required to support these capabilities.
- 3.3.1.5 Implement security capabilities as required to achieve compliance with security laws, rules and regulations.
- 3.3.1.6 Provide assistance with and support to security evaluations, as directed by DIR, which include conducting internal audits, supporting external audits, conducting self-assessments, and evaluating security Incidents.
- 3.3.1.7 Provide assistance with and support to all DIR authorized assessments, develop action plans and resolve deficiencies, vulnerabilities, concerns and recommendations identified within six (6) months of the conclusion of the assessment, as defined in **Exhibit 3.3 Critical Deliverables**.
- 3.3.1.8 Meet all Security-related deliverables and Performance Analytics as defined in **Exhibit 3.1**, which are to be agreed to by DIR and Successful Respondent.

- 3.3.1.9 As requested, attend and contribute to Security Management and Risk Management meetings.
- 3.3.1.10 Resolve agreed actions and activities resulting from Security Management meetings.
- 3.3.1.11 Work with the MSI and contribute to the creation and maintenance of a Security Plan across the Successful Respondent's Services
- 3.3.1.12 Execute Successful Respondent's Security Plan which is agreed to by DIR and coordinated by the MSI.
- 3.3.1.13 Ensure that certificates for Successful Respondent's staff are kept current and report the status to the MSI on a quarterly basis.
- 3.3.1.14 Provide for vulnerability scans for all Successful Respondent network assets, which should include scans for all network addresses at least once per year directly to the DIR Governance, Risk and Compliance (GRC) tool (Currently SPECTRIM) and inform the MSI.
- 3.3.1.15 Provide a forward-looking schedule for the planned Successful Respondent Security testing, assessments and analysis.
- 3.3.1.16 In coordination with the MSI, support the evaluation of new technologies/capabilities for improving security and perform activities and/or solutions to address shortfalls in Security.
- 3.3.1.17 Where investment decisions are required, support the MSI in providing options with associated costs and benefits for DIR review and approval.
- 3.3.1.18 In coordination and support of the MSI, and as related to the Successful Respondent's Services, evaluate details of the Security requirements for new IT services, including options for meeting these requirements and any associated costs.
- 3.3.1.19 Work with the MSI and execute processes according to the governance-approved Master Security Baseline Configuration (MSBC).
- 3.3.1.20 Execute quarterly MSBC Health Checks and run scans quarterly that will feed baseline information to the MSI for the MSI to determine the health check of the systems.

3.3.2 Successful Respondent Staff

The Successful Respondent shall, at a minimum:

- 3.3.2.1 Limit access to data to authorized Successful Respondent personnel only.
- 3.3.2.2 Successful Respondent personnel must have received security clearance and successfully complete a background and criminal history investigation prior to performing contract functions or accessing DIR, DIR Customer Facilities, Systems, Networks or Data.
 - 3.3.2.2.1 Criminal history background checks are to be conducted per Texas Government Code (TGC) Subchapter F, Section 411.1404 and will be in compliance with the then-current versions of the FBI CJIS Security Policy and the FBI CJIS Security Addendum. In addition, an annual background check re-verification is required. DIR must be notified of the compliance with the initial criminal history background check and the annual re-verification.
 - 3.3.2.2.2 Background and criminal history background checks will be performed by the Texas Department of Public Safety and the Texas Department of Criminal Justice. Other

DIR Customers may require additional levels of compliance as per agency regulations and policies.

3.3.2.2.3 Successful Respondent is responsible for any costs associated with the criminal history background check process.

3.3.2.2.4 Successful Respondent will establish a process that facilitates the timely submission and resolution of the criminal history background checks, including but not limited to using digital methods to submit necessary criminal history background check requirements.

3.3.2.3 Implement processes and procedures for tracking Clearances for all Successful Respondent personnel and Third Party Vendors utilizing the Security Clearance Management System provided by the MSI.

3.3.2.4 All work must be performed within the continental US.

3.3.3 Security Incident Management

The Successful Respondent shall, at a minimum:

3.3.3.1 Work with the MSI and contribute to the creation of a Security Incident Management Plan across the Successful Respondent's Services.

3.3.3.1.1 Provide plans and exceptions for all security Incident Management plans including security Incident severity matrix, notification rosters, communications plans, and procedures for managing security Incidents.

3.3.3.1.2 Implement the Successful Respondent's portion of the Security Incident Management Plan in concert with participation from the MSI and required Service Component Providers and DIR Customer personnel.

3.3.3.1.3 Coordinate Security Incident Management procedures with Major Incident Management procedures.

3.3.3.2 Adhere to the security incident handling and notification processes that follow current NIST guidelines and is defined in the SMM.

3.3.3.3 As required, implement and maintain monitoring and alerting services that integrate into the MSI Incident Management System for automated alert notification.

3.3.3.4 Promptly investigate, document, and report security incidents in accordance with 1 TAC Chapter 202 and the SMM.

3.3.3.5 According to the defined process, promptly communicate and escalate security Incidents to the MSI, DIR Customer, and DIR.

3.3.3.6 Conduct Root Cause Analysis and if necessary, develop and implement formal corrective actions or remediation plans once approved by DIR and the appropriate DIR Customer. Evaluate the analysis and proposed corrective actions to ensure future risks are adequately mitigated.

3.3.3.7 Provide Incident investigation support and initiate corrective actions to minimize and prevent security breaches.

3.3.4 Physical Security Administration

The Successful Respondent's shall, at a minimum:

- 3.3.4.1 Communicate the physical and logical security management processes and procedures to Successful Respondent's staff.
- 3.3.4.2 Comply with Successful Respondent physical and logical security responsibilities.
- 3.3.4.3 Inform MSI and DIR Customer immediately if Successful Respondent becomes aware of any vulnerability or weakness in the Services and recommend a solution or mitigation.
- 3.3.4.4 Provide near real-time information, to MSI and DIR Customers to identify those physical access rights that should be removed from MSI and DIR Customer Facilities and where, within the Successful Respondent's scope of responsibilities, initiate the access rights revocation request.

3.3.5 DIR and DIR Customer Sites

Where Successful Respondent uses or visits locations and facilities at DIR and DIR Customer Sites, Successful Respondent shall be responsible for the provision of Services related to DIR Customer's security requirements, set in place by DIR Customer to govern the security of the DIR Customer Environment.

Successful Respondent shall, at a minimum:

- 3.3.5.1 Ensure compliance with all DIR and DIR Customer security policies, standards and procedures, and all applicable laws and regulations, as they may be revised or updated.
- 3.3.5.2 Comply with DIR and DIR Customers' policies, including security, data and records management, and electronic records and data archiving.
- 3.3.5.3 Implement the security-related Services required to protect the confidentiality, integrity, and authenticity of the information stored in or transmitted to or from the DIR Customer environment, in accordance with DIR Customer's security requirements.
- 3.3.5.4 Comply with DIR's, DIR Customers', and Service Component Providers' Physical Security Administration processes, where the processes interact.
- 3.3.5.5 Assist in the development of action plans following any Security Incidents within the DIR Customer environment and implement new controls approved by DIR Customer and in the timeline defined by DIR Customer.
- 3.3.5.6 Maintain DIR Data in accordance with DIR Customer's security policies.
- 3.3.5.7 Establish and maintain safeguards against the unauthorized access, destruction, loss, or alteration of DIR Data in the possession of Successful Respondent in accordance with DIR Customer's security policies.
- 3.3.5.8 Participate in Service Delivery to review any Changes to the Equipment, Software, and networks that potentially have security or operational ramifications and modify the Change to remove or reduce the security or operational ramifications.

3.3.6 Other Locations

Successful Respondent shall, at a minimum:

- 3.3.6.1 Where Successful Respondent uses other locations and facilities to support the provision of Services to DIR or DIR Customers, Successful Respondent's responsibilities shall include the following:

- 3.3.6.1.1 Provide security processes, facilities, Equipment, and Software that meet or exceed DIR's physical security policies, standards, and procedures. Such processes and physical attributes will be at a minimum consistent with similar security provisions maintained by large, well-managed sourcing services companies.
- 3.3.6.2 Upon request, provide DIR, its representative(s), and/or regulatory DIR Customers access to all facilities and assets used in providing the Services for audits, investigations, and compliance reviews.
- 3.3.6.3 Perform all physical security functions (e.g., identification badge controls and alarm responses) at facilities under Successful Respondent's control.

3.3.7 Security Assessments

Successful Respondent shall, at a minimum:

- 3.3.7.1 DIR may initiate and conduct assessments of Successful Respondent's security program. Such assessments will evaluate Successful Respondent's abilities and capabilities in maintaining and enhancing security and safety practices and procedures, and may involve monitoring and testing security programs, conducting risk assessments and performing security design reviews.
- 3.3.7.2 DIR, DIR Customers, Texas State Auditor's Office, and other entities authorized by DIR may conduct security reviews, assessments, forensic analysis and/or audits (e.g., SSAE 18, State Audit Office, IRS audits) where service is being provided by the Successful Respondent. These assessments may include (but are not limited to) physical security, logical security, policies and procedures, network analysis, vulnerability scans and Controlled Penetration Tests.

3.3.8 Assessments

Successful Respondent shall, at a minimum:

- 3.3.8.1 DIR may conduct security assessments, including conducting monitoring and testing security programs (e.g., Controlled Penetration Tests), conducting risk assessments and performing Security Design Reviews, (the "Assessment(s)") of all or any portion of the Services in order to evaluate such Security Program and determine whether the Security Program meets or exceeds the Standard of Due Care.
- 3.3.8.2 Assessments of the Security Program may be conducted by DIR or, at DIR's sole discretion, a third-party security assessment vendor (the "Security Assessment Company").
- 3.3.8.3 The Successful Respondent shall cooperate fully with DIR and/or the Security Assessment Company and provide reasonable access to any premises, equipment, personnel or documents and provide any assistance required by DIR and/or the Security Assessment Company to conduct the Assessment; however, DIR and the Security Assessment Company shall not have access to Successful Respondent proprietary information where it is not relevant to the Assessment, and shall further not have access to confidential or proprietary information of other customers of Successful Respondent than DIR Customers.
- 3.3.8.4 Under no circumstances will Successful Respondent attempt to persuade or control or otherwise influence the Security Assessment Company in the determination of its findings. The Assessment shall be conducted so as not to unreasonably disrupt Successful Respondent's operations under this Agreement.

- 3.3.8.5 Within fifteen (15) days of an Assessment Notice Date, DIR and Successful Respondent will meet to jointly review the relevant Assessment report and if such report concludes that the Security Program does not meet or exceed the Standard of Due Care, then within thirty (30) days after the applicable Assessment Notice Date, the Successful Respondent and the MSI shall develop and agree upon an action plan to promptly address and resolve any deficiencies, vulnerabilities, concerns and/or recommendations identified in such report, consistent with the Successful Respondent's obligations as set forth in the Agreement.

3.4 Request Management and Fulfillment

Successful Respondent shall be responsible for the fulfillment of Service Requests in compliance with processes in the SMM.

3.4.1 Request Management Processes

The Successful Respondent shall, at a minimum:

- 3.4.1.1 Actively participate with the MSI to develop and document processes.
- 3.4.1.2 Actively cooperate with the MSI in implementing and maintaining Request Management and Fulfillment processes that are flexible and facilitate effective communication and coordination across all functional areas.
- 3.4.1.3 Actively cooperate in information exchange between and among the Successful Respondent, the MSI, other Service Component Provider(s), DIR, and DIR Customer to improve end-to-end Request Management.
- 3.4.1.4 Integrate the Successful Respondent's Request Management process with the MSI's Request Management process and systems, where the processes interact.
- 3.4.1.5 Facilitate the automation or mechanization of Service Requests between Successful Respondent and other Service Component Provider(s) systems.
- 3.4.1.6 Facilitate the transparency of Request Management through appropriate processes to provide a complete audit trail for the MSI to meet DIR and DIR Customer legislative and policy requirements.
- 3.4.1.7 Communicate and coordinate the Request Management processes and policies within Successful Respondent's organization.
- 3.4.1.8 Provide effective and agreed upon mechanisms for properly complying with the Request Management Policies.
- 3.4.1.9 Actively participate in developing and establishing Request for Solution processes and appropriate mechanisms to support rapid proposal development that provides a level of accuracy for budgetary information without requiring a full solution.
- 3.4.1.10 Actively support the MSI in establishing processes and workflow for the proper routing of Service Requests.

3.4.2 Service Request Operations

- 3.4.2.1 Actively support the MSI as appropriate to ensure the proper exercise of Request Management activities across all functions and organizations that provide Services to DIR Customers.

- 3.4.2.2 Actively participate in Service Request tracking efforts and provide and maintain regular communications between all parties and Authorized Users through Request fulfillment.
- 3.4.2.3 Manage the effective execution of Request Management for Successful Respondent to achieve its primary purpose to fulfill service requests within the agreed Service Levels and SMM and promote DIR Customer and Authorized User satisfaction.
- 3.4.2.4 Support the MSI to ensure that detailed audit trail information is recorded of all activity that creates, changes, or deletes data and user access to systems that contain DIR and DIR Customer data.
- 3.4.2.5 Engage in effective Request Management governance process to support the MSI in ensuring the following:
 - 3.4.2.5.1 Clearly define and document the type of Service Requests that will be handled within the Request Management process so that all parties are clear on the scope of Service Requests and the Request Management process.
 - 3.4.2.5.2 Establish and continually maintain definitions of all Services, including: descriptions, Services that will be standardized, Services that require custom solutions, and Services that can be requested through each medium (e.g., Service Desk, Portal, Service Catalog, Request for Service).
 - 3.4.2.5.3 Establish and continually maintain Authorized User lists on who is authorized to make Service Requests and type of requests they are entitled to make.
 - 3.4.2.5.4 Communicate to DIR Customers the definition of Services, the Request Management processes, and changes thereto.
 - 3.4.2.5.5 Support regular training for Authorized Users on Request Management processes, Service definitions, and request mediums.
 - 3.4.2.5.6 Perform regular collection of feedback from Authorized Users on the effectiveness of Request Management and engage in activities to improve process and service.
- 3.4.2.6 Support multiple mediums for accepting Service Requests, including the Service Desk, Portal, and Service Catalog.
- 3.4.2.7 Support the use of online self-service to allow Authorized Users to enter Service Requests from a pre-defined list of options.
- 3.4.2.8 Support the provision for real-time visibility of data records associated with Service Requests.
- 3.4.2.9 Update required information on Service Requests within negotiated timeframes to support an up-to-date accurate view of Service Requests.
- 3.4.2.10 Ensure proper approval, including financial authority, or the Service Request through automated means (where practical) prior to Service Request fulfillment.
- 3.4.2.11 Provide and maintain regular communications between all parties and Authorized Users as required until Service Request completion and document the communications in compliance with the Request Management processes.
- 3.4.2.12 The communications frequency shall be determined by the severity of the request and in compliance with the SMM.

- 3.4.2.13 Keep DIR Customer and MSI informed of any issues with the completion of Service Requests and status changes throughout the Service Request lifecycle and in accordance with the SMM.
- 3.4.2.14 Provide anticipated completion times for active Service Requests and update notification systems as required in the SMM to keep DIR Customers and Authorized Users informed in compliance with established Service Levels per **Exhibit 3 Service Levels**.
- 3.4.2.15 Support the MSI to ensure consistent ownership of the Service Request from recording to completion.
- 3.4.2.16 Close Service Requests, in compliance with the SMM, after receiving confirmation from the requesting Authorized User or Successful Respondent support personnel that the Service Request has been completed.
- 3.4.2.17 Track the progress of fulfillment efforts and the status of all Service Requests, including:
 - 3.4.2.17.1 Review the proposed fulfillment time for each Service Request with the appropriate party and update the status accordingly.
 - 3.4.2.17.2 Provide regular updates on the status of all Service Requests within designated timeframes.
 - 3.4.2.17.3 Coordinate Service Request tracking efforts and provide and maintain regular communications, per the SMM, between all parties and Authorized Users until Service Request completion.
 - 3.4.2.17.4 Keep the DIR Customer and Authorized User informed of changes in Service Request status throughout the Service Request lifecycle in compliance with the SMM.
 - 3.4.2.17.5 Keep DIR Customer informed of anticipated Service Request completion times for active Service Requests.
 - 3.4.2.17.6 When a Service Request cannot be completed in the committed timeframe, provide a revised completion time or request a meeting with the Authorized User to determine a new timeframe.
 - 3.4.2.17.7 Track all Service Request completion against the original committed timeframe, regardless of any revisions.
- 3.4.2.18 Utilize the Request Management System provided by the MSI for all Request Management and Fulfillment activities.
- 3.4.2.19 Provide for timely receipt and processing of all requests within designated timeframes from the Request Management System.
- 3.4.2.20 Utilize and update the Request Management System with all relevant information relating to a Service Request.

3.4.3 Request for Solution (RFS)

Requests for Solution (RFS) are those types of DIR Customer requests where requirements are captured in the Successful Respondent's Request Management system and SCP's develop solutions and cost estimates for DIR Customer review and approval. These solutions typically assume the SCP builds and implements the solution. For DIR Customer Requests, which require the Successful Respondent to propose a solution, the Successful Respondent's shall, at a minimum:

- 3.4.3.1 Support the MSI in developing and establishing RFS processes and appropriate mechanisms for the fulfillment of complex requests requiring design, price, solution, and proposals; including appropriate communications to adequately set expectations and promote good customer service.
- 3.4.3.2 Support the MSI in developing and establishing RFS processes and appropriate mechanisms to support rapid proposal development that provides a level of accuracy for budgetary information without requiring a full solution (e.g., rough order magnitude pricing and high-level architecture).
- 3.4.3.3 For all RFS delivered by the Successful Respondent only and that require no other SCP support:
 - 3.4.3.3.1 Review RFS to validate for completeness.
 - 3.4.3.3.2 Coordinate and lead meetings as required to review request, gather requirements, solution and develop the proposal.
 - 3.4.3.3.3 Coordinate the attendance of all necessary subject matter experts in solution and requirement gathering sessions.
 - 3.4.3.3.4 Provide a timeframe for delivering the solution proposal, including cost estimates, once requirements are complete.
 - 3.4.3.3.5 Develop the solution which may include the technical solution, effort, acceptance criteria, solution design document, and pricing.
 - 3.4.3.3.6 Ensure all solutions to requests conform to the DIR-approved architecture, standards, and pricing.
 - 3.4.3.3.7 Ensure all solutions to requests conform the security policies, procedures, and guidelines of DIR.
 - 3.4.3.3.8 Ensure all solutions to requests conform within the bounds and guidelines of DIR Shared Services technical guidelines.
 - 3.4.3.3.9 Coordinate and facilitate solution reviews across the Successful Respondent as required to review and gain approval for the solution and pricing.
 - 3.4.3.3.10 Track all Project Change Requests in accordance with established procedures.
 - 3.4.3.3.11 Provide a single proposal to requesting DIR Customer.
 - 3.4.3.3.12 Iterate and adjust the solution and cost estimating template as required to adhere to the requesting DIR Customer's feedback and requirements.
 - 3.4.3.3.13 Document DIR Customer approvals in accordance with established processes as per the SMM.
 - 3.4.3.3.14 Gather and validate that the proposal acceptance comes from an appropriately authorized user.
 - 3.4.3.3.15 Provide status to DIR and DIR Customers status of all outstanding requests such that DIR Customers can emphasize their organizational priorities.
 - 3.4.3.3.16 Initiate Project Management as appropriate upon proposal acceptance by DIR Customer.
- 3.4.3.4 For an RFS where the Successful Respondent is one of many SCPs, lead and manage the Successful Respondent's solution development and project delivery using the approved

MSI Shared Services Systems and processes and work with the MSI as required to work with the other SCPs to develop a coordinated DIR Customer solution, including:

- 3.4.3.4.1 Effectively execute the RFS processes and appropriate mechanisms for the fulfillment of Successful Respondent assigned requests requiring a solution (e.g., requirements, design, solution, price, proposal) and project delivery (e.g., plan, build, testing, cutover).
- 3.4.3.4.2 Solution the Successful Respondent's portion of the RFS, including:
 - 3.4.3.4.2.1 Participate in meetings as required to review requests, gather requirements, solution and develop proposals with other SCPs, DIR, DIR Customers, and other Third Party Vendors.
 - 3.4.3.4.2.2 Coordinate the attendance of all necessary Successful Respondent subject matter experts in solution and requirement gathering sessions.
 - 3.4.3.4.2.3 Adhere to the MSI provided timeframe for delivering a solution proposal, including cost estimates, once requirements are complete.
 - 3.4.3.4.2.4 Ensure all requests are solutioned within the DIR-approved architecture and standards and pricing.
 - 3.4.3.4.2.5 Ensure all requests are solutioned within the security policies, procedures, and guidelines of DIR.
 - 3.4.3.4.2.6 Ensure all requests are solutioned within the bounds and guidelines of DIR Shared Services technical guidelines.
 - 3.4.3.4.2.7 Participate in solution reviews across the Successful Respondent and all affected SCPs as required to review and gain approval for the solution and pricing.
 - 3.4.3.4.2.8 Contribute to the solution development, cost-estimation, project plan, status, issues and risks in the systems and in compliance with the processes in the DIR-approved SMM.
 - 3.4.3.4.2.9 Support the tracking of all Project Change Requests in accordance with established procedures.
 - 3.4.3.4.2.10 Support the MSI in their development of a single proposal to the requesting DIR Customer.
 - 3.4.3.4.2.11 Iterate and adjust solution and cost estimation as required to adhere to the requesting DIR Customer's feedback and requirements.
 - 3.4.3.4.2.12 Initiate Project Management activities, according to the SMM, upon proposal acceptance by DIR Customer.

3.5 Change Management

The Successful Respondent shall, at a minimum:

- 3.5.1.1 Perform Change Management Services utilizing standardized methods and procedures as defined in the SMM to provide efficient and prompt handling of all Changes.
- 3.5.1.2 Assist DIR Customer in creating the schedule for any Changes and implementing such Changes.

- 3.5.1.3 Assist DIR Customer and MSI to refine and improve upon Change Management processes and training requirements including CAB composition, activities, and the financial, technical, and business approval authorities appropriate to DIR Customer requirements.
- 3.5.1.4 Comply with MSI Change Management processes and training requirements.
- 3.5.1.5 Review and approve refinements to Change Management processes and training requirements.
- 3.5.1.6 Provide necessary information to DIR Customer and MSI to assist in documenting all Request for Change's (RFCs), which could include Change cost, risk impact assessment, and system(s) security considerations.
- 3.5.1.7 Coordinate with DIR Customer to assist in the development of a schedule of planned approved Changes.
- 3.5.1.8 Perform maintenance during regular Maintenance Periods as defined in the SMM, or as scheduled in advance with the approval of DIR Customer.
- 3.5.1.9 Provide Change documentation, as required, to the MSI, including proposed metrics on how effectiveness of the Change might be measured.
- 3.5.1.10 As requested, participate in traditional or digital CAB meetings and workflow to review planned Changes and results of Changes made.
- 3.5.1.11 Utilize the Change Management System, tools, and processes of the MSI for the efficient and effective handling of all Changes, including the CAB, subject to approval from DIR Customer, in a way that minimizes risk exposure and maximizes availability of the Services.

3.6 Asset Inventory and Management

Asset Inventory and Management System provides an inventory of the IT infrastructure managed by the Successful Respondent. The MSI consolidates information from multiple Successful Respondent Asset Inventory and Management Databases that contain details of Equipment, Software, and similar IT service items (collectively referred to as Configuration Items or CIs) used in the provision, support, and management of IT services.

Successful Respondent responsibilities include:

- 3.6.1.1 Actively participate with the MSI to develop and document Asset Inventory and Management processes, as approved by DIR, that document the objectives, scope, and principles that ensure the success of the Asset Inventory and Management processes.
- 3.6.1.2 Integrate Successful Respondent Asset Inventory and Management process with the MSI's Asset Inventory and Management process and systems, including providing Successful Respondent asset data electronically to MSI's Asset Inventory and Management System (AIMS) in the agreed data format.
- 3.6.1.3 Communicate and coordinate the Asset Inventory and Management processes and policies within Successful Respondent's organization.
- 3.6.1.4 Actively cooperate in information exchange between and among the Service Component Provider(s), MSI, DIR and DIR Customer to improve end-to-end Asset Inventory and Management.

- 3.6.1.5 Support the MSI to provide a complete Asset Inventory and Management audit trail to meet DIR and DIR Customer legislative and policy requirements.
- 3.6.1.6 Conform operations to policies and procedures that set the objectives, scope, and principles that ensure the success of the Asset Inventory and Management process.
- 3.6.1.7 Support the MSI in establishing categorization and classification structures to support the proper documentation and maintenance of CIs.
- 3.6.1.8 Use the Asset Inventory and Management process to identify, control, maintain, and verify the CIs approved by the MSI as comprising the Equipment, Software, and Applications to provide the Services.
- 3.6.1.9 Record the CI information for Equipment, Applications, Software and Services.
- 3.6.1.10 Verify that all CIs for the Equipment, Applications, Software, and Services are incorporated into the AIMS.
- 3.6.1.11 Utilize the AIMS provided by the MSI as the single source of information regarding all CIs within Successful Respondent scope.
- 3.6.1.12 Ensure that all CI data related to the Services resides in the AIMS.
- 3.6.1.13 Integrate the Successful Respondent's other systems, including all appropriate and required licenses and/or interfaces with the MSI's AIMS.
 - 3.6.1.13.1 Where Successful Respondent has an internal asset inventory system or database, integrate that system or database with the MSI AIMS as required.
 - 3.6.1.13.2 Provide customization as required to enable the Asset Inventory and Management processes as defined in the SMM.
 - 3.6.1.13.3 Automate processes, discovery tools, inventory and validation tools, enterprise systems and network management tools, etc. to provide electronic Asset Inventory and Management data as required to the MSI.
- 3.6.1.14 Comply with existing and established SMM processes.

3.7 Software License Management

3.7.1 Software License Renewal Management

- 3.7.1.1 Successful Respondent has responsibility for supporting the MSI in tracking, monitoring, and reporting the software renewal process to ensure compliance with software agreements and continued operation of Services. Successful Respondent's responsibilities shall include the following:
 - 3.7.1.2 Comply with the Software License Renewal Management processes, as defined in the SMM.
 - 3.7.1.3 Support Service Requests and Change Requests as appropriate for all renewals and update as needed to reflect the status of each renewal as per the timing and lifecycle process defined in the SMM (e.g., Software expiring in May should be logged as a CRQ in January, 120 days prior to the expiration date).

3.7.1.3.1 Successful Respondent will update the contract data in the approved Software License Renewal System, coordinate with the DIR Customer and MSI to obtain renewal approvals, execute the procurement tasks to renew the software license, install the renewed keys and software, update the Change Request and Contracts data, and log the renewed software keys in the Software License Renewal System as per the process defined in the SMM.

3.7.1.4 In conjunction with the MSI, monitor Software License Renewal progress and SLA achievement.

3.7.1.5 Support the MSI to ensure the requests and Change Requests are completed and closed upon renewal completion.

3.7.2 Software License Compliance Management

3.7.2.1 Support the MSI to determine the compliance position, to monitor and to report the software compliance management process to ensure compliance with agreements and reduce operating risk in the environment. Successful Respondent's responsibilities shall include the following:

3.7.2.1.1 For Successful Respondent provided and managed software, support and execute assigned Software License Compliance Management activities as defined in the SMM.

3.7.2.1.2 For DIR and DIR Customer-retained Software, track and maintain the applicable licensing and use information received from DIR Customers.

3.7.2.1.3 If applicable, utilize tools, such as an enterprise management system and remote monitoring agents, to assist in monitoring efforts, subject to DIR's approval of all such tools.

1. Monitor the Equipment for the presence of any unauthorized or non-standard Software.
2. Define and check for particular Software signatures.
3. Monitor the use of Software developed by the Successful Respondent application development groups.
4. Check the presence and version of Software installed on a particular device and record in the MSI Asset Inventory and Management system.

3.7.2.1.4 Provide reporting of license information and compliance to the MSI, at least quarterly or as directed by DIR.

3.7.2.1.5 Store and track Software license agreements and associated license keys, including processes and procedures for renewals.

3.7.2.1.6 Track license counts and associations within the CMDB.

3.7.2.1.7 Collect and maintain the Contract and Proof of Entitlement (POE) within the MSI-provided system.

3.7.2.1.8 Support the MSI to collect and normalize software titles to standard names.

3.7.2.1.9 Support the MSI to review the Software License Compliance position and determine appropriate remediation.

3.7.2.1.10 Support assigned actions through the Incident, Request, Change, and Project processes for any reported non-compliance of software purchased versus software installed.

- 3.7.2.1.11 Support and provide clarifications about information presented in the Compliance Report to eliminate discrepancies.
- 3.7.2.2 Support the use of Successful Respondent provided and managed Software to maintain strict compliance, including but not limited to:
 - 3.7.2.2.1 Immediately notify and advise MSI of all Software license compliance issues associated with Services.
 - 3.7.2.2.2 Support in the tracking, management and implementation of security certificates used to secure confidential sessions (e.g., SSL) for Internet and Intranet transactions and communications, including processes and procedures for renewals, as required by DIR, DIR Customers, or MSI.
- 3.7.2.3 Support the MSI to confirm the presence and version of Software installed on a particular device and that those attributes are recorded in the MSI Asset Inventory and Management system.
- 3.7.2.4 Support the MSI in reporting of license information and compliance to DIR.

3.7.3 Patch Management

The Successful Respondent shall, at a minimum:

- 3.7.3.1 Be responsible for patch deployment and control of the software and devices under its management.
- 3.7.3.2 Be responsible for participating in DIR Customer Change Management processes to deploy patches on a regular basis.
- 3.7.3.3 Participate in and follow the agreed upon patch rating process.
- 3.7.3.4 Deploy patches to servers and clients per DIR Customer's policies and ensure compliance as required. Use the DIR Customer-approved central deployment tool, as applicable and mutually agreed upon.
- 3.7.3.5 Provide and apply patches to devices within the timeframe guidelines in accordance with DIR Customer's security policies.
- 3.7.3.6 Adhere to DIR Customer's security configuration management.
- 3.7.3.7 Communicate with and/or alert the DIR Customer IT Security team when patches are not installed within the designated timeframe.
- 3.7.3.8 Integrate and have the ability to export patch data associated with all DIR Customer devices.

3.8 Configuration Management

Configuration Management will provide a logical model of the IT infrastructure managed by the Successful Respondent to identify, control, maintain, and verify information related to all Configuration Items that support the Successful Respondent's Services. The MSI consolidates information from multiple Service Component Provider Configuration Management Databases (CMDBs) that contain details of Configuration Items (CIs) used in the provision, support, and management of IT services.

The Successful Respondent shall, at a minimum and as defined in the SMM:

- 3.8.1.1 Actively participate with the MSI to develop and document Configuration Management processes, as approved by DIR, that document the objectives, scope, and principles that ensure the success of the Configuration Management processes.
- 3.8.1.2 Integrate its Configuration Management process with the MSI's Configuration Management process and systems, including providing Successful Respondent Configuration data electronically to MSI's CMS / CMDB in the agreed data format.
- 3.8.1.3 Communicate and coordinate the Configuration Management processes and policies within its organization.
- 3.8.1.4 Actively cooperate in information exchange between and among the Service Component Provider(s), MSI, DIR and DIR Customer to improve end-to-end Configuration Management.
- 3.8.1.5 Support the MSI to provide a complete Configuration Management audit trail to meet DIR and DIR Customer legislative and policy requirements.
- 3.8.1.6 Conform operations to policies and procedures that set the objectives, scope, and principles that ensure the success of the Configuration Management process.
- 3.8.1.7 Support the MSI in establishing categorization and classification structures to support the proper documentation and maintenance of CIs.
- 3.8.1.8 Use the Configuration Management process to identify, control, maintain, and verify the CIs approved by the MSI as comprising the Equipment, Software, and Applications to provide the Services.
- 3.8.1.9 Record all Successful Respondent's CI information including, but not limited to, equipment, software, applications and relationships to applications, software, services, and equipment.
- 3.8.1.10 Verify that all CIs supporting the Successful Respondent's Services including Equipment, Software, and Services are incorporated into the CMDB.
- 3.8.1.11 Utilize the CMDB provided by the MSI as the single source of information regarding all CIs within Successful Respondent scope.
- 3.8.1.12 Ensure that all configuration data related to the Services resides in the CMDB.
- 3.8.1.13 Integrate the Successful Respondent's other systems, including all appropriate and required licenses and/or interfaces with the MSI's Configuration Management System(CMS).
 - 3.8.1.13.1 Where Successful Respondent has an internal CMS, integrate that system with the MSI CMS as required.
 - 3.8.1.13.2 Where Successful Respondent has an internal CMDB integrate that database with the MSI CMDB.
 - 3.8.1.13.3 Provide customization as required to enable the Configuration Management processes as defined in the SMM.
 - 3.8.1.13.4 Automate processes, discovery tools, inventory and validation tools, enterprise systems and network management tools, etc. to provide electronic asset and configuration management data as required to the MSI.
- 3.8.1.14 Comply with existing and established SMM processes.

3.9 IT Service Continuity Management

Successful Respondent is responsible for maintaining an IT Service Continuity Management (ITSCM) plan for its own internal staff and systems to respond to an emergency and continue to provide Services to DIR and DIR Customers.

The Successful Respondent shall, at a minimum:

- 3.9.1.1 Develop, maintain, and test Disaster Recovery Plans (DRPs) and Technical Recovery Guides (TRGs) as defined in the SMM for the Systems, Software, and Equipment used by Successful Respondent to provide the Services, including those provided at the Consolidated Data Centers, DIR Customer Service Location, or other Successful Respondent Facilities.
 - 3.9.1.1.1 The DRPs and TRGs should comply with all applicable Federal and State requirements.
- 3.9.1.2 In the event of a disaster, recover and support affected Systems, Software, and Equipment at the designated recovery location according to the agreed Recovery Time Objective (RTO) and Recovery Point Objective (RPO) in support of the Service Levels defined in **Exhibit 3.0 Performance Model**.
- 3.9.1.3 Coordinate Successful Respondent's ITSCM plan with MSI ITSCM plans and DIR Customer Business Continuity Plan (BCPs) to ensure DIR Customers can resume regular business functions in the event of a Disaster or significant event affecting the Systems, Software, and Equipment used by Successful Respondent to provide the Services.
- 3.9.1.4 In the event of a service disruption, coordinate all ITSCM efforts to ensure smooth and efficient resumption of Services.

3.9.2 Crisis Management

Crisis Management may be necessary, depending on the type of business or geographic location where Services are being performed, in the event of hurricanes, tornados, riots, terrorist threats, etc. The Successful Respondent shall, at a minimum:

- 3.9.2.1 Following MSI, DIR, and DIR Customer notification processes for any crisis event occurring in or relating to a Successful Respondent Facility, DIR Facility, or other facilities managed by Successful Respondent in connection with the Services.
- 3.9.2.2 Following statewide notification pyramid alert support as documented in the applicable business continuity plan.
- 3.9.2.3 Coordinate with MSI, DIR, and DIR Customers requirements for Services that are critical to designated DIR Customer emergency management responsibilities.
- 3.9.2.4 Coordinate with MSI, DIR, and DIR Customer regarding variances in Services as a result of Crisis Management in compliance with all SMM procedures.

3.10 Project Management

Project Management provides a way to execute and manage projects with the goal of delivering projects from request through completion, meeting DIR Customer requirements in terms of timing, quality, and cost.

The Successful Respondent shall, at a minimum:

- 3.10.1.1 Be responsible for executing and project managing projects related to the Successful Respondent's Services.
- 3.10.1.2 Conform Successful Respondent operations to MSI-defined policies and procedures to ensure the success of the Project Management process.
- 3.10.1.3 Use the MSI provided Project and Program Management (PPM) system as the single source of project management and information regarding all projects and programs.
- 3.10.1.4 Ensure that all Successful Respondent Project Management data resides in the PPM system.
- 3.10.1.5 Execute projects according to the approved Program Management and Project Management methodology as defined in the SMM.
- 3.10.1.6 Projects that meet the criteria for "major information resources project", as defined by Texas Government Code 2054.003 (10), are subjected to state Quality Assurance Team (QAT) oversight requiring the Successful Respondent to support the following:
 - 3.10.1.6.1 Adhere to the requirements and guidelines as outlined in the Project Delivery Framework located here:
<http://dir.texas.gov/View-Resources/Pages/Content.aspx?id=16>
 - 3.10.1.6.2 Provide project deliverables as required for the QAT to review and provide proactive monitoring of project outcomes.
 - 3.10.1.6.3 Develop and execute corrective action plans for projects with QAT identified project risks.
 - 3.10.1.6.4 Provide status reports to the MSI and DIR as required to report to QAT stakeholders (state leadership, DIR leadership, DIR and MSI project teams).
 - 3.10.1.6.5 Escalate significant issues to the MSI and DIR and advise on alternative methods for correction.

3.11 Release Management

The purpose of Release Management is to build, test and deliver specified Services that will accomplish the stakeholders' requirements and deliver the intended objectives.

The Successful Respondent shall, at a minimum:

- 3.11.1.1 Work with the MSI and other Service Component Providers(s) to develop and establish a Release and distribution process so that each change to Service Provided Services is controlled, tested, traceable, authorized, and implemented in a structured manner.
- 3.11.1.2 Conform Successful Respondent operations to the agreed Release policies, processes and procedures as defined in the SMM.
- 3.11.1.3 Execute releases according to the approved Release Management methodology as defined in the SMM.
- 3.11.1.4 Use the MSI provided Release Management System as the single source of Release Management and information regarding all Successful Respondent Releases.

4 BUSINESS MANAGEMENT

4.1 Operational Intelligence

Successful Respondent shall provide the data and/or reports to the MSI for report creation and posting via the MSI-managed Operational Intelligence System and Portal as specified in **Exhibit 3.4** Description of Reports. Service Level reports are defined in **Exhibit 3** Service Levels, and operational reports are defined in **Exhibit 3.4-A Reports**.

The Successful Respondent shall, at a minimum:

- 4.1.1.1 For core Services, provide online reporting capability with near real-time data for use by DIR Customers in the generation of sophisticated, custom reports.
 - 4.1.1.1.1 As agreed with DIR, coordinate with the MSI to provide single sign-on access to Successful Respondent's reports through the MSI Portal.
- 4.1.1.2 As appropriate, provide near real-time operational data feeds to the MSI-managed Operational Intelligence System.
- 4.1.1.3 Provide on-time, monthly service-level performance data for each Service Level requirement, to the MSI-managed Service Level Management System.
- 4.1.1.4 Provide mutually agreed upon reports and data to the MSI to enable invoice reconciliation.
- 4.1.1.5 Coordinate with the MSI and provide data to support the creation of integrated performance dashboards. Dashboard data should support:
 - 4.1.1.5.1 Near real-time health dashboards for any Systems managed by Successful Respondent highlighting status of health metrics as defined by DIR Customer.
 - 4.1.1.5.2 Report monthly, quarterly, and annually in the Security Dashboard on the deployment of Tools and procedures to the DIR Customer Environment.
- 4.1.1.6 The Successful Respondent shall be responsible for using DIR's security governance, risk and compliance system to provide information relevant to the service offering, including but not limited to risk assessments, Incident reporting, and security plan development.
- 4.1.1.7 As required, collaborate with other Texas.gov Service Component Providers, to include sharing reports and information via the MSI Portal or other mutually agreed upon mechanism as appropriate to ensure effective Service delivery.
- 4.1.1.8 Support integration of applicable security Service solutions, in which data from multiple sources (e.g., scan results, multiple IDS platforms/IPS devices, and MDS devices) are incorporated and integrated into the Service.
- 4.1.1.9 Provide ad hoc and summary Security Incident Reports to DIR OCISO using security systems and data generated in accordance with the format and content of the then current version of 1 TAC Chapter 202.

4.2 Service Level Management

Service Level Management includes the activities associated with managing and reporting attainment of Service Level performance, deliverable commitments, and customer satisfaction. The Successful Respondent shall, at a minimum:

- 4.2.1.1 Provide accurate and timely SLA data to the MSI, as defined in **Exhibit 3** Service Levels, and the SMM.

- 4.2.1.2 When SLAs fail to meet minimum, or expected service level targets, implement Service Level Improvement Plans (SLIP), as described in the SMM.
- 4.2.1.3 Analyze DIR Customer Scorecard feedback to understand DIR Customer issues and develop and execute issue resolutions.
 - 4.2.1.3.1 Collate information provided to Successful Respondent from End Users (e.g., captured in Service Desk surveys, feedback through emails) regarding suggested improvements to the Services.
 - 4.2.1.3.2 Develop an action plan to address suggested improvements to the Services identified by Successful Respondent and DIR Customer, including the following:
 1. Provide the action plan to DIR Customer for review.
 2. Implement DIR Customer-approved action plans.
 3. Report in the Dashboard on progress and improvements made on approved action plans.
- 4.2.1.4 Summarize and report on plans and activities that affect the overall Services to MSI and DIR governance boards.

4.3 IT Financial Management

Successful Respondent must provide IT Financial Management Services in support of the **Exhibit 4** series.

The Successful Respondent shall, at a minimum:

- 4.3.1.1 Actively work with the MSI to develop and document IT Financial Management processes.
- 4.3.1.2 Actively cooperate in information exchange between and among the MSI, DIR, and DIR Customer to improve end-to-end IT Financial Management.
- 4.3.1.3 Facilitate the transparency of IT Financial Management through appropriate processes to provide a complete audit trail for the MSI to meet legislative and policy requirements.
- 4.3.1.4 Integrate Successful Respondent IT Financial Management process and system with the MSI's IT Financial Management process and system, where the processes interact, and as agreed to with DIR and the MSI.
- 4.3.1.5 Actively support the MSI to assure the proper application of IT Financial Management across all functions and organizations that provide services to DIR Customers.
- 4.3.1.6 Communicate and coordinate the IT Financial Management processes and policies within Successful Respondent's own organization.
- 4.3.1.7 Utilize the IT Financial System provided by the MSI such that it serves as the single source of information regarding all IT Financial Information for Services within Successful Respondent scope.
- 4.3.1.8 Integrate Successful Respondents' systems and chargeback data with the MSI IT Financial System, including providing all appropriate and required licenses and/or interfaces.
- 4.3.1.9 Provide sufficient data and detail to support DIR and DIR Customers State and Federal funding accounting, grant, and audit requirements.

- 4.3.1.10 Collect, aggregate, and provide billing, service provisioning, and service metric information to the MSI as required.
- 4.3.1.11 Identify unique DIR Customer account identifiers to identify Applications, Application Instances, and other services information as required.
- 4.3.1.12 Provide the MSI with monthly invoice data required for the MSI to render the Successful Respondent statement of Services.
 - 4.3.1.12.1 Support all charges with detailed invoice data as required in **Exhibit 4.3 Form of Invoice**, and supporting utilization data at the DIR Customer, Resource Unit, Charge Category (e.g., Programs, Divisions, Organization Units) as required by the MSI.
- 4.3.1.13 Actively participate in developing and maintaining the processes for the resolution of invoice disputes within designated timeframes.
- 4.3.1.14 Provide effective and agreed mechanisms for crediting DIR Customers as appropriate.
- 4.3.1.15 Effectively execute the processes to record, track, and manage incidents of invoice disputes.
- 4.3.1.16 Research and review invoice disputes for completeness and supporting data accuracy, and, when necessary, request clarifying data from DIR Customer.
- 4.3.1.17 Support and initiate additional treatment of invoice disputes to facilitate resolution within designated timeframes.
- 4.3.1.18 Ensure that incidents of invoice disputes are continually updated, at a minimum on a weekly basis.
- 4.3.1.19 Keep the MSI informed of activity and anticipated resolution times for active incidents of invoice disputes.
- 4.3.1.20 Allow DIR to monitor and validate invoice dispute process on an ongoing basis.
- 4.3.1.21 Provide a process for escalating to Successful Respondent management incidents of invoice disputes not resolved within the time frames established within DIR policies.
- 4.3.1.22 Provide data and support to enable the MSI to report on all Texas.gov transactions and revenue, including, at a minimum:
 - 4.3.1.22.1 Provide application transaction and financial transaction data to the MSI to support the MSI provided Financial Management System functionality to allow for near real-time reporting of the Texas.gov transaction and payment details including reports as required to fully reconcile all attempted and failed transactions.
 - 4.3.1.22.2 Provide customer, application and transaction data to the MSI as required to support the MSI provided reporting on transactions and payment data by type of transaction, application, customer, etc.
 - 4.3.1.22.3 Provide the required data to the MSI with the appropriate level of detail to enable the MSI to link all application and payment engine generated revenue to each individual transaction.
 - 4.3.1.22.4 Provide the required data to the MSI to enable the MSI to invoice DIR Customers for Texas.gov fees.

4.4 Capacity Management

Capacity Management assesses the current operations and future demands, pre-empting performance issues by taking the necessary actions before they occur.

The Successful Respondent shall, at a minimum:

- 4.4.1.1 Integrate Successful Respondent Capacity Management process and agreed data with the MSI's Capacity Management process and systems, including providing Successful Respondent Capacity data electronically to MSI's Capacity Management System in the agreed data format.
- 4.4.1.2 Communicate and coordinate the Capacity Management processes and policies within Successful Respondent's organization.
- 4.4.1.3 Actively cooperate in information exchange between and among the Service Component Provider(s), MSI, DIR and DIR Customer to improve end-to-end Capacity Management.
- 4.4.1.4 Provide the means to automatically aggregate resource and system performance, system utilization, capacity limits for Successful Respondent Services.
- 4.4.1.5 Provide the means to automatically calculate and forecast Successful Respondent Services capacity requirements through trending of collected data anticipating capacity needs.
- 4.4.1.6 In an automated manner, aggregate capacity information including current capacity and utilization, trends, issues and actions at the DIR Customer and Services level.
- 4.4.1.7 Initiate Incident Management, Problem Management or Request Management activities as needed to address Capacity Management issues and trends.
- 4.4.1.8 Action and track agreed capacity mitigations through associated Incidents, service requests, changes or projects using the MSI provided systems.
- 4.4.1.9 Participate and contribute to Capacity Management meetings.
- 4.4.1.10 Incorporate appropriate capacity modeling to extrapolate forecasts of growth and other changes in response to projected DIR Customer business and operational needs.
- 4.4.1.11 Provide meaningful Capacity Planning input to the MSI-coordinated Capacity Plan.
- 4.4.1.12 Provide meaningful Capacity Planning input to the Technology Plan in support of requirements for long-range planning.
- 4.4.1.13 Provide meaningful Capacity Planning input to the Refresh Plan in support of Refresh and Technical Currency.

4.5 Refresh and Technical Currency

Operating software, database software, and application utility tools are required to be within n or $n-1$ of the currently supported versions of the software manufacturer.

4.5.1 Refresh Responsibility

The Successful Respondent will work with the MSI to ensure that refreshes are done as scheduled and technical currency is maintained in the Services. Successful Respondent's responsibilities include:

- 4.5.1.1 Maintain application currency and ensure the developed application software will support the DCS standard hardware and software platforms as described in the DCS Standard Configurations.
- 4.5.1.2 Upgrade and replace Equipment and Software (“Refresh”) as required in **Exhibit 4.2 Financial Responsibility Matrix** throughout the Term, for purposes that include meeting DIR’s and DIR Customers’ business requirements; preventing technological obsolescence or failure; and accommodating volume changes, the ability to increase efficiency, the ability to lower costs, and/or the need to maintain the required Third-Party Vendor support.
- 4.5.1.3 Cooperate and coordinate on-going Refresh activities with the full Refresh Program at the direction of the MSI.
- 4.5.1.4 Deploy Equipment and Software associated with any Refresh in accordance with the standards of DIR’s technical architecture and the Technology Plan.
- 4.5.1.5 Accommodate the timeframes and other requirements associated with Refresh, as well as the financial responsibility for the underlying assets, as provided in **Exhibit 4.2 Financial Responsibility Matrix**.
 - 4.5.1.5.1 DIR reserves the right to modify the Refresh timeframes and requirements during the Term based on its business requirements, subject to the Change Control procedures.
- 4.5.1.6 Cooperate, report, and support the management of Refresh Responsibilities by the MSI.
- 4.5.1.7 Where the Successful Respondent is financially responsible for Equipment and Software used in conjunction with the Services, as listed in **Exhibit 4.2 Financial Responsibility Matrix**, Successful Respondent’s responsibilities include:
 - 4.5.1.7.1 Refresh the assets during the Term, including responsibility for the assets, the implementation, and ongoing support.
 - 4.5.1.7.2 At a minimum and/or in the absence of a defined Refresh timeframe, maintain technical currency in accordance with Industry Standards.
- 4.5.1.8 Where DIR and Customers are financially responsible for Equipment and Software used in conjunction with the Services, the Successful Respondent will implement and support the new assets provided by DIR.
- 4.5.1.9 Regardless of the ownership of underlying assets, Successful Respondent responsibilities include:
 - 4.5.1.9.1 Provide personnel who are adequately trained in the use of the Equipment or Software to be deployed as part of the Refresh, and provide such training prior to the Refresh.
 - 4.5.1.9.2 Provide minimal disruption to DIR’s and Customers’ business operations associated with technology Refresh.
 - 4.5.1.9.3 Use best practices and effective automation tools during Refresh deployment.
 - 4.5.1.9.4 Perform all Changes to Equipment and Software in accordance with Change Management procedures.

4.5.2 Technology Refreshment and Replenishment

Technology refreshment and replenishment (**TR&R**) Services are the activities associated with modernizing the Applications on a continual basis so that the system components stay current with evolving industry-standard technology platforms. The following list identifies the TR&R Services that Successful Respondent will perform.

- 4.5.2.1 As part of its responsibilities, recommend TR&R life cycle management policies, procedures and plans appropriate for support of Customer's business requirements.
- 4.5.2.2 Assist DIR, Customer, and MSI with developing TR&R plans that meet requirements, and adhere to STC Customer policies.
- 4.5.2.3 Assist DIR and Customer with the necessary tasks required to implement the TR&R plans.
- 4.5.2.4 Provide management reports on the progress of the TR&R plans to DIR, Customer, and MSI.

4.5.3 Software Currency and Release Levels

Successful Respondent's responsibilities include:

- 4.5.3.1 Monitor "end-of-life" hardware and software processes resident in each Successful Respondent's technology plan and ensure proper notification is provided to DIR, Customer, and Third-Party Vendors regarding support and software currency plans.
- 4.5.3.2 Unless otherwise directed by DIR, provide and support Software under Successful Respondent's operational responsibility at the most recently released and generally available version of the Software (the "N" release level).
- 4.5.3.3 As directed by DIR, also support releases as specified in **Exhibit 4.2 Financial Responsibility Matrix**.
- 4.5.3.4 Use commercially reasonable efforts to support Software that is no longer supported by the Third-Party Vendor.
- 4.5.3.5 Provide support for all Software versions and release levels that exist as of the Effective Date until otherwise directed by DIR.
- 4.5.3.6 Provide monthly reports of upcoming software releases, software renewals and end-of-support notices on affected DIR Customers to the MSI, at least 180 days prior to expirations date.

4.5.4 Refresh Planning

The Successful Respondent will work with the MSI to ensure refresh planning is consistently done and in compliance with processes outlined in the Service Management Manual. Successful Respondent's responsibilities include:

- 4.5.4.1 Develop a continual plan for Refresh, including:
 - 4.5.4.1.1 Within one-hundred and twenty (120) days prior to DIR's annual planning process meetings, review the asset inventory and produce a report that lists the assets that are due to be refreshed in the upcoming plan year, and provide such report to DIR's annual planning process.
 - 4.5.4.1.2 Cooperate and participate in the planning activities led by the MSI.
 - 4.5.4.1.3 Successful Respondent and DIR will consider the usability of the assets and review alternatives to replace, re-lease, consolidate, or retain the assets. Based on the results

of this review, Successful Respondent will deliver the initial recommendations regarding such assets to DIR within thirty (30) days after the review.

- 4.5.4.1.4 For Successful Respondent-owned assets, Successful Respondent and DIR will mutually determine whether Successful Respondent will replace an asset and the appropriate replacement date.
 - 4.5.4.1.5 If Software Changes are required due to replacement of assets, Successful Respondent, in consultation with the DIR, will review alternatives for making changes to such Software.
 - 4.5.4.1.6 Such replacement of the assets and Software will be at Successful Respondent's expense if the replacement is required to facilitate achievement of the agreed upon Service Levels or because the asset is obsolete (i.e. replacement parts cannot be acquired or the asset has become unserviceable).
 - 4.5.4.1.7 For DIR and Customer owned and leased assets, based on the planning process outcome and direction established by DIR, Successful Respondent will provide a proposal for refresh of those assets (replacement at DIR's expense) to DIR.
- 4.5.4.2 Adhere to DIR's approved plan, and execute that plan utilizing established procurement processes, to initiate refresh and retirement activities.
- 4.5.4.2.1 Provide monthly reports 180 days prior to lease expiration date showing assets to be refreshed with latest data.
 - 4.5.4.2.2 Notify DIR monthly of all open agreements related to assets that are retired or will retire within 180 days of the report date.
- 4.5.4.3 Track and report on the completion progress of asset Refresh.
- 4.5.4.4 Update and archive asset records after retirement.